2005

The recognition and application of security risk management in corporate governance

Chris J. Cubbage
Edith Cowan University

Edith Cowan University

Copyright Warning

The recognition and application of

Security Risk Management in Corporate Governance

By

Chris J. Cubbage

A thesis submitted to the
Faculty of Communications, Health and Science
Edith Cowan University, Joondalup

In partial fulfillment of the requirements for the degree
of Bachelor of Science (Security) with Honours

Principal Supervisor: Professor Narayanan SRINIVASAN

Submission Date: 30 September 2005

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

Abstract

Security as a profession and discipline has emerged principally in the later half of the twentieth century and has developed to become a more defined, usual, respectable and visual part of management. This study aimed to determine the degree of recognition and application of security risk management to corporate governance practices in Australia.

Formal research design used descriptive research methodology, consisting of a literature review, primary document analysis and a questionnaire survey to collect data. This research was contrasted to a *Corporate Governance Security Model* formulated to determine if the model is applicable to the recognition, or application, of a security function to the Australian Stock Exchange ('ASX') Corporate Governance principles.

A major finding of this study is that security functions and responsibilities are poorly recognised and documented by Australia's largest public company boards. A majority of directors will have no experience or qualifications in security risk management and this is likely to be reflected down through the organisation resulting in low to medium security awareness and culture.

Corporate governance statements from companies listed on the ASX/S&P 200 strongly suggests that security related risks are not widely considered as part of the corporate governance framework. With limited application of security in the corporate governance framework, there is less focus on security related behaviour within the codes of conduct held by a majority of public companies. This can have an adverse impact on corporate ethics, internal controls and crisis response capabilities.

The study developed a model which implements security risk management functions to the corporate governance framework in order to formally recognise and promote effective management of security risk and compliance. Applying security as a business process to support long term revenue was found to benefit corporate reputation and compliments other risk and business management practices. Security of information and confidentiality is enhanced to encourage reports of misconduct within the company, generating a security and reporting culture.

Security functions are currently limited to form part of internal controls within the operating environment and generally viewed as a cost centre which does not contribute to revenue. Security functions are not holistically applied across the organisation or within the corporate governance framework.

There are a number of recommendations resulting from the study and are primarily concerned with the continued need for research into the application and recognition of security within the hierarchy of executive and business management.

Declaration

I certify that this thesis does not, to the best of my knowledge and belief:

i. Incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

ii. Contain any material previously published or written by another person accept where due reference is made in the text; or

iii. Contain any defamatory material.

Date 18/10/2006

Acknowledgements

My most sincere appreciation in conducting and completing this study goes to the senior faculty group of ECU Security Science, School of Mathematics and Engineering. In particular, Professor Nara Srinivasan, Associate Professor Dr. Clifton Smith and Course Coordinator Mr. David Brooks for their support and encouragement.

Thanks also to Professor Bob Officer, Associate Professor Iain Watson and Mr. Athol Yates for assisting in the pilot study.

I would especially like to thank my family who has sacrificed many hours of quality time as a result of vocational commitments added with studies. Ironically, one undertakes study in pursuit of professional fulfillment to sufficiently provide for one's family.

Definition of Terms

Awareness	A measure of knowledge of existence, including recognition and recall of key features or positioning.
Board of Directors	Director Group with ultimate responsibility for managing a company and determines strategy and sets policies and expectations for implementation.
Corporate Governance	Non-prescriptive, self-regulatory principles and practices to protect stakeholder interests and promote improved long term company performance.
Critical Infrastructure	Physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period,

	would significantly impact on social or economic well-being.
Culture	A system of shared values, assumptions, and norms which unite and influence behaviour.
Risk	The chance of an occurrence which will impact upon an activity or objective.
Risk Management	Involves managing risk to achieve an appropriate balance between realising opportunities for gains while minimising losses.
Security	An implied stable and predictable environment without disruption, harm or fear of destruction or injury.
Security Function	The process and systems in place to stabilise an environment and protect against disruption, harm and fear of disruption or injury.

Security Environment	The measure of the environment's stability and predictability resulting from the security function.
Terrorism	Premeditated, politically or ideologically motivated violence perpetrated against public targets by groups or agents, intended to harm and influence.

Table of Contents

ABSTRACT III

DECLARATION IV

ACKNOWLEDGEMENTS V

DEFINITION OF TERMS VI

TABLE OF CONTENTS IX

LIST OF FIGURES XII

LIST OF TABLES XIII

CHAPTER 1 1

INTRODUCTION 1

BACKGROUND 1
SIGNIFICANCE OF THE STUDY 3
PURPOSE OF STUDY 4

RESEARCH QUESTION 5

CHAPTER 2 6

LITERATURE REVIEW 6

CORPORATE THEORY 6
CORPORATE GOVERNANCE 8
Failures in Corporate Governance *10*
ROLE OF THE BOARD 13
THE SECURITY FUNCTION IN CORPORATE GOVERNANCE 22
Position of security in the organisational hierarchy *22*
Security Risk Management *28*
Crisis and disaster recovery planning *42*
Security culture *50*
Codes of Conduct *57*
Communicating security *59*

CHAPTER 3 **62**

THE STUDY **62**

STUDY PROCEDURE 62
Design *63*
SAMPLES AND SUBJECT SELECTION 65
DOCUMENT ANALYSIS 66
RESEARCH INSTRUMENTS 67
Questionnaire *67*
CORPORATE GOVERNANCE SECURITY MODEL 70
PILOT STUDY 70
ETHICAL CONSIDERATIONS 71
LIMITATIONS 72

CHAPTER 4 **74**

STUDY RESULTS **74**

STATISTICAL CALCULATIONS FROM DOCUMENT ANALYSIS 76
QUESTIONNAIRE RESULTS 81
STATISTICAL CALCULATIONS FROM QUESTIONNAIRE 81

CHAPTER 5 **86**

DATA ANALYSIS AND INTERPRETATIONS **86**

CHAPTER 6 **91**

STUDY OUTCOMES AND RECOMMENDATIONS **91**

RESEARCH CONCLUSIONS 91
RESEARCH RECOMMENDATIONS 94

CHAPTER 7 **97**

CONCLUSION **97**

REFERENCES 100

BIBLIOGRAPHY 107

ANNEXURE 1 - APPROACH TO QUESTIONNAIRE RESPONDENT 109

ANNEXURE 2 - STUDY INTRODUCTION WEBSITE & QUESTIONNAIRE 110

ANNEXURE 3 - CORPORATE GOVERNANCE SECURITY MODEL 116

ANNEXURE 4 - DOCUMENT ANALYSIS OF ASX LISTED COMPANIES 119

List of Figures

Figure 1:	Risk management's ability to generate profit.	39
Figure 2:	Levels of security communication.	60
Figure 3:	Sector Profile of Target Population.	75
Figure 4:	Target Population's disclosure of a Risk Management Committee.	76
Figure 5:	Percentage of corporate governance policies concerning environmental risk.	77
Figure 6:	Percentage of corporate governance policies concerning occupational health and safety risk.	77
Figure 7:	Percentage of corporate governance policies concerning asset protection.	78
Figure 8:	Percentage of corporate governance policies concerning a security function.	79
Figure 9:	Percentage of corporate governance policies concerning reporting policy.	80

List of Tables

Table 1:	Document Types examined.	74
Table 2:	Sector Profile of Target Population.	74
Table 3:	Sector Profile of Target Population completing questionnaire.	81
Table 4:	Responses to Questionnaire Part 1.	82
Table 5:	Responses to Questionnaire Part 2.	83
Table 6:	Responses to Questionnaire Part 3.	84
Table 7:	Responses to Questionnaire Part 4.	85

CHAPTER 1

Introduction

Background

> HIH has been central to the whole corporate governance debate as a glaring example of what can go wrong when a company makes it look as though it has good governance, when in fact it has almost none (Main, 2003, p. 269).

Australia has had some prominent corporate crises in recent years, including HIH, One.Tel, Harris Scarfe, Ansett and Pan Pharmaceuticals (Ferguson, 2003, p. 40). In 2001-02 the number of complaints to the Australian Securities and Investment Commission ('ASIC') concerning corporate governance and administration grew 12.8% from the public and 42% from external administrators, who include auditors, liquidators and receivers (Ferguson, 2003, p. 35). Serious complaints include the leaking of information from confidential board meetings. An example is an information leak to the Sydney Morning Herald within hours of a NRMA Board meeting in 2002. ASIC referred the matter back to the company highlighting that they considered the complaint to be an internal corporate governance matter. The leak is estimated to have cost NRMA members up to $5 million (Ferguson, 2003, p. 5).

In light of these Australian cases, as well as cases in the United States ("U.S.") and United Kingdom, corporate governance has become a major corporate issue. New legislation has been introduced in Australia aimed at tightening

company disclosures on executive remuneration and increasing penalties for continued breaches of disclosure obligations. Stephen Matthews, the Australian Shareholders Association deputy chairman asserts that "Boards and their CEO's have a long way to go to restore shareholder faith and trust" (Elliott, 2003, p. 33). The United States have also introduced new legislation, the *Sarbanes-Oxley Act 2002* which requires extra oversight of auditing processes, elimination of conflicts of interest and greater corporate transparency (Mills, 2003, p. 1).

Furthermore, in response to international terrorism events, the Australian Government is calling on businesses who are owners or operators of critical infrastructure to begin exchanging key data on their threats, vulnerabilities and business continuity planning (Dearne, 2003).

It is the determination of individual businesses and organisations to take responsibility for their own corporate governance and infrastructure protection (Dearne, 2003). As new global and business risks emerge, new approaches are required to identify and treat those risks.

Security as a profession and discipline has emerged principally in the later half of the twentieth century and has developed to become a more defined, usual, respectable and visual part of management (McCrie, 2001, p. 15). In comparison with the boom of Information Technology (IT) in the late 1990's and early this century, global terrorism, electronic crime and corporate collapses appear to be supporting a similar demand in the security and risk management sector.

Significance of the study

This study is significant and well timed as corporate governance and security are two of the major issues concerning the corporate world today. The two issues are brought together in this study.

Corporate security directors or managers should have a sound understanding of corporate governance principles to ensure the security function is integrated into the corporate governance framework. Primarily, corporate security should be ingrained into the company's risk management and preferably there should be a seat for the security champion on all risk management committees.

The significance of this study is based upon its implications to current corporate governance and security risk management practices in Australia and overseas. Should the study confirm security's enhancement of the corporate governance framework, and a model with which it can be implemented, it will provide new approaches to current corporate governance policy, and promote security as a valued business practice at executive management and board level.

The study will also generate more interest in security management research and education, particularly in its application to business leadership and executive management. This will contribute to the continued growth and acceptance of the security profession.

Purpose of Study

Thematic research priorities for the protection of the built environment, including critical infrastructure, proposed by Yates (2004, p. 10), state that challenges related to business awareness of the changed security environment and risk management include;

a) A failure to integrate security considerations into governance frameworks;
b) Lack of business awareness that sound business risk management, security and resilience can be a long term revenue enhancer;
c) Lack of benchmarks and metrics for effective security investment;
d) Lack of integration of security into the issues of consideration for all professionals and managers;
e) Lack of risk management and security risk experience in business; and
f) Lack of modeling tools and validation models.

This study, in line with Yates' research priorities, researches security's role in corporate governance and endorses the progression of security as a profession. The study presents a *Corporate Governance Security Model* to which a security function can be recognised or integrated in the current corporate governance and risk management framework recommended by the ASX Corporate Governance Council (2003). The study proposes security guidelines, which are applicable to the governance of public and private companies.

By demonstrating that security risk management enhances corporate governance, this study supports the security function as a viable and necessary business framework that contributes to core business and profit generation. The *Corporate Governance Security Model* promotes best practice security management and supports security as a necessary contributor in corporate assessment, particularly risk management, auditing and business continuity.

Research Question

Refer to Annexure 3: Corporate Governance Security Model

1. Does the *Corporate Governance Security Model* recognise an existing security function in current corporate governance practices?
2. Does the security function proposed by the *Corporate Governance Security Model* enhance current corporate governance practices?

CHAPTER 2

Literature Review

Corporate Theory

According to Dine (2000, p. 3) theories of company existence are all important in the understanding of the appropriate corporate governance model. Three theories which have been influential in shaping models of companies are; contractual, communitaire and the concessionary theories. "The contractual and communitaire theories represent two extremes since they reflect notions of the company as a product of laissez-faire individualism and as an instrument of the state, respectively." Concession theory is considered the middle ground.

Concession theory accepts the state's role of ensuring corporate governance structures are fair and democratic, and the notion that the company should realign itself to reflect the social aspirations of the state would be opposed. In its simplest form, concession theory views the existence and operation of the company as a concession by the state, which grants the ability to trade using the corporate tool (Dang, 2000, p. 21).

Bottomley (cited by Dang, 2000, p. 23) proposes the term 'corporate constitutionalism' which is the acceptance that the state has a legitimate role in regulating corporate governance. Corporate constitutionalism has three key

features; "the idea of dual decision-making, which recognises the different roles of the board of directors and the general meeting of shareholders in corporate life; the idea of deliberative decision-making, which seeks to ensure that corporate decisions are made on the basis of an open and genuine consideration of all relevant issues; and the idea of a separation of power, which aims to make corporate decision-making power diffuse and accountable."

It is through pricing decisions which providers of funds signal their assessment of the quality of governance, which should in turn provide an incentive to the owners of the enterprise to alter the quality of governance (Jain, 2000, p. 231). In efficient market theory (Kaen, 2000), corporate problems will be solved and company officers would act in a manner consistent with the interests of all stakeholders. Long term consequences will be priced at an appropriate discount and result in the flow of funds through investment. In an efficient market, financial crisis is more likely to happen due to unforeseeable and uncontrollable events.

However, the reality is a highly competitive international market, which is unlikely to exhibit all the traits of efficiency, all of the time. Competition for funds can lead to behaviours by company officers that challenge a fair market, and result in activities which ignore long term consequences, considering only the short term horizon. In what appears rational from the respective of the individual director, may end up as appearing irrational for the market as a whole (Jain, 2000, p. 234).

Corporate Governance

Corporate governance is an established global issue, and whilst it differs between markets internationally, on matters of principle they are converging. Dunlop (2001, p. 45) asserts that recent literature is focusing "on the need for the adoption of non-prescriptive self-regulatory governance principles to promote improved performance, unlike earlier material which emphasized prescriptive, regulatory solutions. Governance has moved from a '*trust me*' to a '*show me*' environment."

Corporate governance essentially exists due to the separation of ownership and control, due to the interests of those who maintain control over the corporation differ from the interests of the members and those who supply it with external finance. Corporate governance is the method of reconciliation between the two to ensure that businesses are run in the interests of all stakeholders, but particularly the shareholders (Png, 2001, p. 156).

Corporate governance encompasses the relationships and patterns of behaviour between different agents in a limited liability corporation. It refers to the rules and practices which frame the interactions between the corporate managers, shareholders, employees, creditors, key customers and communities (Burgeat, 2001, p. 3; Kaen, 2000, p. 247).

Corporate governance is the creation and implementation of processes which seek to optimise the return to shareholders whilst satisfying the legitimate

expectations of stakeholders. It presupposes that the board, and therefore the company, will act consistently within a declared set of values against which its actions can be judged (Cassidy, 2003, p. 34).

Dunlop (2001, p. 47) proposes a need for a dynamic governance model with four main requirements being '*building trust*', '*earning freedom from excessive regulation*', '*investor performance*' and '*flexibility in governance*'. There is no proof that any one model results in optimum performance and it needs to be recognised that an appropriate governance model will vary between companies, and over time, for the individual company (Dunlop, 2001; Bosch, 1995).

According to Bosch (1995, p. 65) it is argued that increased international competition from Japan, Europe and newly industrialised Asian economies, caused pressure on U.S. companies to improve corporate governance to strengthen their international competitiveness.

> Good corporate governance is a key to establishing a robust and competitive corporate sector, which serves as a source of economic growth (Burgeat, 2001, p. 3).

Corporate governance is an important element in a company's contribution to international competitiveness. Whilst minimum international standards must be met, Australia should be using corporate governance performance to gain a global competitive advantage. "Rather than slavishly following international practice, we should be seeking governance innovations to this end (Dunlop, 2001, p. 48)."

Corporate governance in Australia has adopted and learned from the experience of other countries and in turn has served as a model for other countries. Bosch (2001, p. 5) asserts that there is a "wide gap between the maximum possible and the minimum excusable, and the whole spectrum is observable in Australian corporate governance...There are many directors who regard board membership as more a matter of prestige and social intercourse than of serious duty."

Failures in Corporate Governance

The first well documented failure in governance was the South Sea Bubble in England in the 18th century. In 1929, the stock market crash resulted in the U.S. reforming securities regulation that led to federal legislation in 1933 and 1934. Recent events in the 1980's and 1990's, such as the collapse of Bank of Credit and Commerce International, Barings Bank and the economic crisis of South East Asia and Russia, resulted in a call for greater governance and supervision. These major incidents were often the result of incompetence, fraud and abuse (Png, 2001, p. 155).

Poor corporate governance was identified as one of the root causes of the recent Asian financial crisis (Burgeat, 2001, p.3; Jain, 2000, p. 232). Nam, Kang and Kim (2001, p. 85) found that illegal practices of breach of trust, expropriations and embezzlement, and company theft appear to continue in many East Asian countries, but the punishment of such abuses remains largely weak.

Ellett (2000, p. 173) suggested that Australia has a very weak system of ensuring companies are adopting best practice in corporate governance. The Australian Stock Exchange (ASX) regulates corporate governance practices via the Listing Rule 4.10.3. These rules state that the company must make a statement of the main corporate governance practices that it has in place during the reporting period. There is no mandatory compliance with any specified benchmarks.

The ten (10) essential corporate governance principles recommended by the ASX Corporate Governance Council (2001, p. 14) are;

Principle 1 - Lay solid foundations for management and oversight;

Principle 2 - Structure the board to add value;

Principle 3 - Promote ethical and responsible decision-making;

Principle 4 - Safeguard integrity in financial reporting;

Principle 5 - Make timely and balanced disclosure;

Principle 6 - Respect the rights of shareholders;

Principle 7 - Recognise and manage risk;

Principle 8 - Encourage enhanced performance;

Principle 9 - Remunerate fairly and responsibly; and

Principle 10 - Recognise the legitimate interests of stakeholders.

Sarre (2001, p.299) confirms that whilst most corporations voluntarily comply, there remains concern over the failure of Australian companies to meet international standards of best practice. There is evidence of a lack of conformity and uniformity, and the suggestion that the ASX requirements are simply used as

a means of maintaining legitimacy and control, not necessarily to allay stakeholders' concerns. Hiliary (cited by Sarre, 2001, p. 300) asserts "that many entities view the rules as a means of avoiding the threat of litigation, and overlook the broader accountability objective of satisfying the need for public disclosure in order to promote stakeholder confidence."

Confidence in corporate governance can first be enhanced by the disclosure of the role, responsibilities and methods of appointment of the board of directors, second, the responsibility for the strategic direction, day-to-day management and internal controls, and third, director remuneration (Dunk & Kilgore, 1998, p. 146).

Seven million people own shares in Australia's 1500 listed companies. Corporate governance will continue to evolve as a result of genuine widespread retail concern about capital markets. A company should be encouraged to engage in greater dialogue with investors about the company's sound corporate governance practices to differentiate it from competitors, to showcase how objectives are met, how risks are managed and how performance is reviewed for improvement (Hamilton, 2004).

The review of practices, which have remained, unchanged or unchallenged may lead to better practices that maximise value. At worst, an informed confidence is provided about the existing board and management (Hamilton, 2004).

Dunk and Kilgore (1998, p. 157) found that managers realise that shareholders are better informed than they were ten years ago, and 89 per cent of respondents reported that shareholders now demand more information than they did ten years ago.

The external appearance of corporate governance entails a network of public policies and regulatory institutions that present a level playing field and compliance with rules. Transparency is the essence of corporate governance and the protection of the rights of investors and shareholders (Adekunle, 2003, p. 171).

> There is little value in a checklist approach to corporate governance that does not focus on the particular needs, strengths and weaknesses of the company (ASX Corporate, 2003, p. 8).

There is no single model for good corporate governance and practices will evolve with the changing circumstances of the company and developments in Australia and overseas. Business decisions always carry risks that require effective management through oversight and internal controls. Enhanced board and management effectiveness come from keeping pace with the modern risks of business (ASX Corporate, 2003, p. 6).

Role of the Board

The board of directors ensures the company has a suitable chief executive and management team in place, and reviews the direction in which it proposes to take the company, working through any management changes along the way. To

do this effectively, the board must understand the risks and opportunities facing the organisation (Hansell, 2003, p. 5).

Until the 1990's academic textbooks on business management gave little attention to the role of the board. There were no courses in business schools on corporate governance, and the first dedicated book on corporate governance, in Canada, was not published until 1992 (Hansell, 2003, p. iii). Bosch (1995, p. 7) confirms that training courses concentrated on technical and managerial areas, rather than on the duties of directors, and developments only began in the late 1980's.

Attention on the duties of directors have also been aided by progressive court judgments, since the 1990's, which have interpreted director's duties more stringently, placing more onerous and exacting legal responsibilities on company directors. Court cases which have arisen include those dealing with health, safety and environmental protection. Directors must identify the issues which need to be addressed by the board, they must deal with their responsibilities, and record their decisions clearly (Bosch, 1995, p. 41).

Leader (cited by Dang, 2000, p. 188) argues that directors "are obliged to decide issues by identifying the personal and derivative rights of corporate stakeholders, giving paramountcy to the derivative rights that equate to the ongoing health of the company as a viable concern."

Chow (1996) (cited in Dunk & Kilgore, 1998, p.146) emphasised that the need for management and the board to achieve sound financial performance ranked within the practice of sound corporate governance. Chow argues that institutional investors are unlikely to simply invest in a well governed company if its financial performance is poor, and therefore the focus of such performance will be on short-term measures.

The two basic duties a director has to the company are a fiduciary duty and a duty of care, both powerful legal concepts. Courts are likely to deal harshly with directors who act contrary to one or both of these duties, but will show restraint in questioning decisions made by directors which are consistent with these duties. The theory of these duties, cited by Hansell (2003, p. 97) is "that if each director adheres to the appropriate standards of loyalty and care, board decisions which are properly motivated and appropriately thoughtful will follow."

In Australia, company directors and other officers have legal obligations, civil and criminal, pursuant to sections 180 to 184 of the *Corporations Act 2001*. The civil obligations, pursuant to sections 180 to 183 are to act with care and due diligence, act in good faith, not to improperly use their position to gain an advantage or cause a detriment, and not to improperly use information. They are criminally responsible, pursuant to section 184, if they are reckless or intentionally dishonest and fail to discharge their duties in good faith in the best interests of the corporation or for a proper purpose (Corporations Act, 2001).

Increased accountability at the board level can present the board with difficult strategic decisions concerning the direction of an organisation, what obligations it should enter into and what kind of alliances or partnerships are appropriate. In its monitoring role, the board has to be satisfied that all its obligations are met (Fishel, 2003, p. 7).

The ultimate responsibility for managing a company rests with the board and it is the board that determines how involved it should be in management. Hansell (2003, p. 49) proposes that "the functions of the board and management result from the styles and personalities of the individuals who comprise the board and the management team as well as the challenges which the corporation faces over time."

The board sets the ethics policies and expectations of the company, however it is the Chief Executive Officer ('CEO') who sets the tone which will influence day-to-day behaviours. Directors should be independent enough to inquire or discuss whether the CEO's behaviour demonstrates honesty and integrity. Boards should be alert to any indications that the CEO, other company officers, or directors, are not conforming to the company's code of conduct (Cole, 2004).

The role of a board is determined by the type of model the board functions within. Boards shouldn't confine themselves to rigid methods, but be flexible in their approach, sliding back and forth across a scale of engagement as issues and circumstances do. The five models proposed by Nadler (2004, p. 9), are;

1. The *passive board*, considered a traditional model, provides limited accountability, with the board's main function to ratify management decisions. "The board's activity and participation are minimal and at the CEO's discretion";
2. The *certifying board* emphasises credibility to shareholders and the importance of independent directors. The board oversees orderly succession plans, certifies management processes and ensures the CEO meets the board's requirements;
3. The *engaged board* provides insight, advice and support on key decisions with the CEO. The board conducts substantive discussions on company issues and clearly defines its role and boundaries;
4. The *intervening board*, commonly used in crisis, becomes deeply involved in key decision making, and holds more frequent, intense meetings; and
5. The *operating board* is considered to have strong, ongoing board involvement, making key decisions for management to implement. Commonly used in early stage business startups, where the board or top executives have specialised expertise but lack management experience.

Boards can be packed with must-accomplish items to allow an in-depth examination of any one. Directors must overcome frustration to dig deeper into meatier subjects, such as strategy, planning and risk management. Frustration can be caused by poor communications between senior management and the board. Effective ways in which senior management can keep the board in the

dark is by providing too little information, or by providing too much (Nadler, 2004).

In Nadler's (2004, p. 12) study, he found that only 28 per cent of the directors surveyed had independent channels for obtaining useful information about their company. They rely on management to share the necessary information, or which it chooses to share. Other boards suffered from feeling that information was missing or that they were being prevented from doing their jobs.

Boards are often provided with two sources of information. The first is retrospective data and trailing indicators of company performance and operations. The second is presentations by the CEO and senior management about the interpretation of financials and the continued vision of the company. Nadler (2004, p. 12) asserts that "Given those meager rations, it's no wonder companies get into deep trouble before their boards find out."

Hansell (2003, p. 9) asserts three elements of a board's decision; the information it has available to it; the process it uses to consider that information; and the business judgment it applies to that information in the context of that process. Effective directors take positive steps to inform themselves about the industry and broader environment within which the company operates. Directors should not be dependant on management as the only source of information, otherwise external developments are only considered from the perspective of management (Hansell, 2003, p. 11).

Cohen and Grace (2001, p. 116) assert that accountability is important, but more narrow a notion than responsibility. Responsibility is proactive, involving the use of discretion and exercising sound judgment. To make decisions, one has responsibility and one is to be held accountable for the decisions made.

The board retains the responsibility of ensuring appropriate policies are in place, and since circumstances are continually changing, it is likely that they will become outdated, and therefore periodic review is essential (Bosch, 1995, p. 97). "Being complacent is not a good business decision (Business Executives, 2004, p. 25)."

The board has a monitoring function which includes the oversight of the risk management process. The board should re-evaluate risk and related risk management strategies on a regular basis. In opposition to corporate risk management is corporate chance management, with the taking of risks an essential part of the business process and of transactions. The primary role of directors is to identify and benefit from business chances when they present themselves (Hansell, 2003, p. 6).

A Booz Allen and Hamilton survey (cited by Bosch, 1995, p. 125) of directors of major Australian companies showed that 77 per cent of respondents agreed that "substantial scope exists for improving the practices of boards'.

Australian company boards typically meet 12 times a year with an average meeting time of five hours (Bosch, 2001, p. 5). Carter (cited by Buffini, 2004) asserts that there is a widening 'expectation gap' between what the public expects and what directors can realistically do. Directors must review the business strategy and approve budgets, monitor business performance, evaluate the chief executive, approve large investments and dividends, oversee management succession planning, approve executive remuneration, ensure major risks are identified and managed, ensure accuracy of financial reporting and oversee the management of general and legal compliance. "That's quite a job for a few weeks in a year". Boards may become risk adverse with the constant pressure for companies to perform and criticism of directors when they don't.

Mansell (cited by Pownall, 2004, p. 14) disagrees with the view that boards are resistant to change, instead boards are very keen to do as well as they can. The mix around the board table is also changing, with those becoming directors having the appropriate track records and experience, but not necessarily knowing the others around the table.

Wolnizer (1994) (cited by Dunk & Kilgore, 1998, p. 148) proposed that there is a widespread expectation that audit committees improve the standards of corporate governance by, amongst others, aiding in reducing fraud and misconduct by creating an environment of corporate discipline and control that

effectively reduces the opportunity for such practices, improving the effectiveness of both the internal and external audit function.

Collier's (1997, p. 104) study into audit committees found that the subjects dealt with by the audit committees were fairly consistent with the main subjects being the examination of major accounting problems, critical accounting decisions, adequacy of disclosures and major audit problems. In addition, the committee considered the nature and scope of the audit, issues raised by the auditors, action taken on management concerns and any major control issues. Collier also determined that having at least one non-executive director with an accounting qualification was extremely useful, but the presence of non accounting members was also important, as different questions are asked which occasionally provides new insights (Collier, 1997, p. 105).

An audit committee concerns itself with what has happened in the company. A risk management committee should be aligned to look ahead at what may happen to the company. Company management should concentrate on reducing risks, but also know what level of risk is consistent with the business. Rather than turning operational managers in to risk managers, it is more productive for them to have risk management procedures, which advises them on areas of risk which may impact their operations (Lawson, 2004).

A KPMG study (cited by Buffini, 2004) of the top 50 ASX listed companies, and 18 mid-sized companies showed that all had audit committee and risk

management policies, 96 per cent had clearly defined the different roles of directors and management, and most had required charters, policies and codes of conduct. However, only 66 per cent had a majority of independent directors, one in two audit committees weren't properly constituted, less than 20 per cent reported that their CEO and Chief Financial Officer ('CFO') had signed off on accounts, and only 47 per cent reviewed their own performance.

The security function in corporate governance

Position of security in the organisational hierarchy

Amoroso (cited by Broersma, 2004) asserts that "For any company, it is virtually impossible to ensure protection of assets without one person owning the focal point."

A study by Cavanagh (2004b) surveyed nearly 100 chief executive and company officers in a wide range of mid-sized (annual revenues between USD$20 million and USD$1 billion) companies in the U.S.. The proposal that security provides value for the firm and a positive return on investment was endorsed by 61 per cent of respondents, with 39 per cent regarding security as a cost which must be tightly controlled.

Survey results relating to contact between chief executives and security chiefs showed that only 21 per cent met at least once a week and 25 per cent met at least monthly. In the remainder, 28 per cent met only a few times a year and 26 per cent had never met with the security chief at any time during the previous year (Cavanagh, 2004b).

Corporate security should be ingrained into the company's risk management and preferably there should be a seat for the security champion on all risk management committees. One of the primary endeavors of the *Corporate Governance Security Model* is to integrate security risk management into the day to day management of the company, and ensure direct access to the CEO and other executives, as and when required.

Access to the CEO by the security officer has a direct impact on security spending. 75 per cent of companies which held weekly meetings with the security officer reported an increase in security spending since 9/11, compared to 30 per cent of those firms where there were no meetings. In companies with monthly meetings, 30 per cent reported security spending increases of more than 10 per cent, compared with 19 per cent of companies with occasional meetings, and 9 per cent of companies with no meetings (Cavanagh, 2004).

Strongest support for security spending, according to Cavanagh's study, was in 'critical industries' which include transportation, energy, utilities, financial services, media and telecommunications, information technology and healthcare.

Following the September 11, 2001 terrorism attacks, 45 per cent of respondents reported no increase in security spending and most reported little increase.

Increases in security spending was lowest amongst smaller companies. Only 28 per cent of mid-sized companies have off-site emergency operation centres. Cavanagh (2004) proposed from the study that many smaller American companies would have difficulty conducting business in the event of a prolonged power outage or closure of their primary facility.

Cavanagh's (2004) study found that the smaller the company, the less likely its board of directors is to establish written security guidelines, and less likely to have procedures in place to handle security situations. 71 per cent of mid-sized companies had board approved written guidelines on disaster recovery and business continuity. Only a third reported board approved, written policies dealing with routine security issues.

Cavanagh (2004b) asserts that "articulating and championing the business case for security must be seen as an essential part of the role played by any corporate security director." This may be more difficult if security is not directly reporting to top management, however as security concerns become more integrated into strategic management, this should improve.

A role for the security discipline on the board and within corporate governance frameworks should be to compensate, not contribute to, asymmetric concern in dealing with risk management and crisis management. Company failures and debacles are generally not random events, they are the result of failures in governance, that grew out of the nature of the business, and the nature of human beings. Governance mechanisms must be rooted in an understanding of human nature (Tschoegl, 2000, p. 117). The security discipline should provide the board with the experience needed to perform rationally under stress, and to balance company protection with company officer entrepreneurialism and self interests.

Corporate security directors or managers must have a sound understanding of corporate governance principles to ensure the security function is integrated into the corporate governance framework. Strong holistic security controls which are reported regularly to the board and designated committees, will enable alert watch-keeping of director, management and employee behaviour, operational security and loss mitigation monitoring, asset protection strategies and external forces, all which can cause critical stress on short and long term financial performance. Corporate scandals, like that of HIH, have been caused by the reliance on trusted directors or employees to do the right thing. It has been repeatedly shown that they do not always do it (Walter, 2000, p. 37).

Senior management experience is likely to become an important qualification as the role of a security director moves up "the food chain" in corporate significance. Currently, security is mostly placed in mid-level management positions, which is

a modest level given the current international environment (Cavanagh, 2004a, p. 6). The highest levels of the organisation, the Board of Directors and its operating committees must be provided with the strategy, costs and related impacts of the security function, and the nature and probability of catastrophic and significant security risk events (ASIS International, 2004).

It would seem that as social responsibilities increase and the nature of protective challenges evolve, the current demarcations in corporate responsibilities tend to blur. Operations, finance, information technology, human resources, property, purchasing and security departments all have a stake in creating and maintaining the best possible risk reduction and mitigation plans. Many companies have already turned their Health, Safety and Emergency (HSE) managers into HSE and Quality (HSEQ) managers. Other companies have turned theirs into HSE and Security (HSES) managers. One company in Singapore has a position termed CRASHES, responsible for Community Relations, Auditing, Security, Health, Emergency Response and Safety (Hayes & Truscott, 2004, p. 37).

Developments in the U.S. have created the position of a Chief Security Officer ('CSO'), intended to be analogous to the 'C-suite', like that of the CEO, CFO and the Chief Information Officer ('CIO'). The CSO's role is to coordinate all security responsibilities throughout the organisation, report to top management and the board, and control the security budget, so security spending can be managed more effectively. The CSO concept places accountability on a single person to oversee the many aspects of security operations and allows for better

coordination and dissemination of information across the company (Cavanagh, 2004a, p. 15). This provides an integrated security strategy with less duplication and lower cost (ASIS International, 2004).

Allison (cited by Cavanagh, 2004a, p. 27) asserts that "...security professionals must be comfortable in the governance arena as well as in operations...They must also be able to articulate the case for security measures that affect overall company policy and operations. The business protection challenge is huge."

ASIS International CSO Guidelines (2004, p. 9) propose that the CSO must have the skills to accomplish the following;

- Relate to and communicate with senior executives, the Board of Directors and operating committees;
- Understand the strategic direction and goals of the business, and how security intertwines with strategic needs;
- Understand and assess the impact of external and internal changes on security risk;
- Ensure security and related ethical issues are appropriately investigated and resolved with limited impact on business operations;
- Facilitate the use of traditional and advanced scenario planning techniques for senior management, the Board of Directors and employees;
- Successfully network and develop working relationships with external and internal resources;
- Promote organisational learning and knowledge sharing;

- Be politically astute, but not politically motivated;
- Be realistic and comprehend the need to assess financial, employee and customer implications in plans and recommendations;
- Function as an integral partner of the senior management team; and
- Develop sound organisational security awareness, which is appropriate for the business and organisational culture.

Security Risk Management

There are varying forms of risk and they include credit risk, liquidity risk, market risk and operational risk. Operational risk encompasses management fraud, failure of computer systems, human error, failure of safety systems, and most relevant in this text, security failures (Harper, Keller & Pfeil, 2000, p. 5).

Academic finance and management literature has paid attention to risk management of market and credit risks, but has largely ignored operational risk, which includes *inter alia*, problems with information systems, operational problems, breaches in internal control, fraud and unforeseen crises. Tschoegl (2000, p. 104) asserts that "...there are almost no articles dealing with misbehaviour in organizations."

A survey by the Institute of Internal Auditors (cited by Gettler, 2004, p. 42) held that only 13 per cent of Australian CFO's considered the ASX Corporate Governance Guideline's (2003) requirement to sign off on risk management

strategies would have a positive impact on the company. Only 20 per cent were in favour of having external auditors verify their risk management controls.

ASX Listing Rule 4.10 deals with corporate governance disclosure practices in the form of Guidance Note 9 (2001). Item 8 specifically deals with '*business risk*', and "*the board's approach to identifying areas of significant business risk, and to putting arrangements in place to manage them*". Guidance in risk management refers to Standards Australia 'Risk Management' AS/NZS 4630 (1995).

A 2003 Connect 4 survey (cited by Fenton-Jones, 2004) determined that Australia's top 200 listed companies increased spending on audits by 10 per cent to $175 million. The increase was attributed to an increase in dealing with corporate governance compliance issues. Revenue of board advisory services increased by 60 per cent over the previous two years. Risk management in particular was seen as the main compliance issue.

The Cadbury Committee Working Group (cited by Mills, 1997, p. 124) defines internal controls as;

> ...a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories – effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations (Cadbury Committee Working Group, 1993).

Mills (1997, p. 124) asserts, based on the Cadbury definition, that internal controls should be embedded into the entity's activities, and through their integration, provide quality control, prevent unnecessary costs, and protect the company against unwelcome surprises. Dang (2000, p. 145) upon analysis of the collapse of Barings Bank, asserts that "internal controls are vital".

Risk assessment and management, forming part of internal controls and corporate governance, can be seen in a positive vein because a value-creation framework offers much potential for drawing together many key corporate governance issues from a holistic perspective (Mills, 1993, p. 139).

In Mills' (1993) study into internal control practices within large UK companies, 76.9 per cent responded that their internal controls were not restricted to financial ones. Only 13.8 per cent and 6.9 per cent responded that the effectiveness of their internal controls was interpreted as resulting in reducing risk of material loss and reasonable assurance that company's assets are safeguarded, respectively (Mills, 1993, p. 132).

Risk analysis is used to highlight schemes where profitability is subject to greater than normal uncertainty, so that attention can be drawn to areas requiring closer control. Appleby (1987, p. 82) asserts that both sensitivity and risk analysis complement one another in their approach to reducing uncertainty in strategy and tactics.

Most companies today, particularly larger public companies, can demonstrate extensive and at times, impressive risk management systems, however these generally relate to financial risks, market risks, credit risks, workplace safety and environmental risks. In contrast, the greatest risks have been shown to be the willful and ignorant misconduct of employees and management. Unethical and criminal misconduct is often difficult to detect and can directly result from organisational culture (Walter, 2000, p. 34).

Ealy (1993) (cited in Mills, 1993, p. 128) proposes that risk management ensures earnings and assets are protected and that it is particularly important for it to be integrated with top management and corporate strategy. Porter's (1992) Five Forces and Value Chain Analysis recognised that risk can arise at the entity-wide or activity level.

Risk needs to be identified and managed, not only financial risks, but also other risks which could affect the company's future as a going concern. The Cadbury Committee Working Group proposed that to achieve this, directors should be constantly aware of the external environment in which the company is operating (Mills, 1993, p. 129).

Mills (1993) study also sought to identify how companies define and assess business risk. 56.6 per cent of respondents defined risk as an event or occurrence which may have a significant effect on the operational or financial stability of the group. Only 6.7 per cent defined security of assets as a key risk.

Mills found that management were most likely to give attention to risks that impacted on immediate profitability and cash flow. This is consistent with a previous study (Marsh, 1991) in which it was found that greater concern was shown to short-term factors and longer-term strategic issues were seen as less important (Mills, 1993, p. 135).

Company stakeholders expect the board and executive management to identify and anticipate areas of risk and have in place a holistic strategy to mitigate or reduce those risks. The expectation extends to management responding in a highly effective manner to events and incidents which threaten the assets and earnings of the company. The continued monitoring and mitigation of risk and loss is the responsibility of the governing board and senior management, and provides a positive impact to profitability (ASIS International, 2004; Cromie, 2004, p. 21).

Clarke and Dean (2001, p. 80) stated that the dominant similarity between the major Australian corporate failures over the last five decades is the 'surprise' response to the disclosure of the company's distress.

Provisions for taking 'all reasonable care' as found in environmental protection and occupational health and safety legislation, is applicable to a security function. Taking all reasonable care serves as a process in which directors and management put in place systems and procedures necessary to enable the corporation to comply with statutory and industry obligations, and to monitor the

operation of those systems to ensure that they continue to achieve compliance objectives (Hansell, 2003, p. 144).

Class action litigation in the U.S. has seen courts alter the legal definition of a 'forseeable event' to indicate that a 'terrorist act' and computer viruses and worms are forseeable events. In action brought against airlines, airport security companies and airplane manufacturers following 9/11, the court determined that "the danger of a plane crashing if unauthorized individuals invaded the cockpit was a risk that the plane manufacturer should reasonably have foreseen". Computer viruses were determined to be foreseeable due to the number, and regularity, of bulletins issued by software companies regarding viruses, worms and computer attacks (Cook, 2004).

The author proposes that significant business risks have emerged in the current climate of international terrorism, reviews of critical infrastructure protection and growth in sophisticated, transnational organised and electronic crime. Current corporate governance guidelines recommend that these *significant* risks should be managed in accordance with AS/NZS 4630 however, complimenting models should also be investigated.

> It remains to be seen if the usual ways of doing business will prove adequate to the challenge of managing corporate security in an increasingly threatening international environment (Cavanagh, 2004a, p. 5)

The following recent events highlight the emergence of significant security related business risks and include, or support, calls for security guidelines to be integrated in to corporate governance practices;

- The Commonwealth Attorney-General's Department, in concert with other Australian Government agencies with responsibilities for critical infrastructure protection is seeking to strengthen relationships with owners and operators of the nation's critical infrastructure in the form of the Trusted Information Sharing Network (TISN) (Yates, 2004, p. 15).
- New maritime counter-terrorism standards are being enforced by the U.S. through the International Maritime Organisation. Countries and maritime related businesses failing to meet security standards risk having their ships and exports turned away from U.S. ports (Pitsis, 2004, p. 4).
- The Australian Institute of Criminology estimates that consumer-based internet fraud is between 5 to 10 per cent of all online transactions. The National Office for the Information Economy estimates about 1.5 per cent of all credit card sales over the internet is fraudulent. All merchants must now meet new EMV smart card standards by 2006 (Fenton-Jones, 2003, p. 47).
- Australia's four major banks (Commonwealth Bank, ANZ Bank, National Australia Bank and Westpac Bank) were criticised for failing to clearly warn and equip online banking customers of hoax emails and websites perpetrating online banking frauds (Moullakis, 2004, p. 5).
- Australian on-line betting sites have been targeted by Russian extortion gangs, who have effectively closed the sites down by flooding them with

traffic, after the companies refused to pay extortion money (Legard, 2004). The U.S. is also seeing an escalation of cyber-extortion attacks targeted at e-commerce companies (Vijayan, 2004).

- The US National Counterintelligence Executive reported that in 2001 the combined costs of foreign and domestic economic espionage, including intellectual property theft, was US$300 billion. All companies must carefully review their security policies (Gengler, 2003, p. 7).
- Mroz and Conner (2003, p. 6) argue that cybersecurity is a business and corporate governance issue that must be addressed by corporate chief executives and boards of directors. What is lacking is a corporate governance framework that allows effective execution.
- The 2003 Economic Crime Survey determined that 'Economic Crime' is a significant threat and found that one third of respondents stressed the company's board had ultimate responsibility for preventing or managing economic crime, but only just over a quarter had given their boards any risk management training (Economic Crime Survey, 2003, p. 3).
- The Australian National University has introduced a new master's course elective titled "*Security in Business and Government*" as the university perceived there was no course on offer in Australia that looked at protective security from a senior management perspective (Williams, 2003, p. 13).

Warning signs prior to the collapse of large companies, such as HIH, were shown to have been ignored, misunderstood or were not sufficiently communicated to

force pre-emptive action by the board. Warning signs included concerns raised by regulators, downgrading of credit ratings and conference papers (White, 2001, p. 59). Applying such a warning to the security environment, the author proposes signs such as threats and attacks to Australian interests from terrorist groups, national intelligence agency issues, sustained increase in fraud and computer crime, and warnings from international security, police and military experts of impending terrorist attacks in Australia.

In this context, security's fundamental task, as part of risk management and the corporate governance framework is to;

1. Identify security risk from consultation with management and outside advisors;
2. Evaluate risks to determine appropriate security management strategies;
3. Review the risk management strategy to satisfy themselves with the way management proposes to manage each of the principal risks;
4. Monitor the security management process from management reports which should describe major occurrences or less significant occurrences which suggest a trend; and
5. Take remedial action of any material breach of the controls or pattern of immaterial breaches, discuss with management the remedial action required, and monitor the implementation and effectiveness of any action taken (Hansell, 2003, p. 6; Pausenberger & Nassauer, 2000, p. 265).

The *Corporate Governance Security Model* (Annexure 3) demonstrates how the security function can be applied to the recommended corporate governance practices to enhance performance outcomes. The outcomes proposed by the model are;

1. The board recognises its responsibility for security risk management and security compliance and control;
2. The board accepts security as a profession and seeks specialist advice on security issues when necessary;
3. Security behaviour and risk management is recognised and practiced within the board and corporate culture;
4. Security controls are maintained and reviewed by the board;
5. Security risk management is recognised by the board as a long term revenue enhancer;
6. Security related risks are managed for disclosure of 'sensitive' information; and
7. Shareholders are ensured that the company's physical, information and electronic security and integrity is maintained.

The security function at a board and executive level can enhance corporate governance by identifying security and risk management opportunities, formulate strategic security and protection policy, and manage operations to improve and protect returns on investments, supporting the principle of shareholder optimisation.

Duncan, Gale, Tofflemore and Yaksick (1992, p. 7) argue that in light of security's ability to maximise shareholder value, security risk management in corporations should be viewed as a specialised application of financial management. They define security risk management as activities associated with making and implementing investment decisions in anticipation of or following contingent losses.

The objective of security is to protect and enhance all asset types, and therefore expenditures on security constitute investments in the organisation. By adopting corporate finance theory in security management, a security investment methodology identifies strategies that maximise the net present value of the investment (Duncan et al, 1992, p. 12).

It is the security director's role to ensure that corporate security management is effective, and does not waste resources on security items the company does not need, or may not need at the time. The provision of sound security analysis and management proposals to the board and executive management allows the company to consider and approve a balanced security plan. This promotes efficient spending to reduce 'under' or 'over' investment in security systems, and provides board approved security procedures to counter risks which can severely impact the company's reputation, intellectual and physical assets, and its ability to recover from crisis.

The application of security to corporate governance should involve the board or designated committee formulating the security policy of the organisation and developing appropriate security practices and culture. Strategic security planning should be in line with corporate direction and key resources, directing the board and executive management in protecting all asset types, mitigating loss and providing accountability for corporate governance.

Measurement of the security function should be based on the economic value added to the organisation following effective and balanced security and business protection strategies which has shielded principle business. Rewards to all stakeholders come from sound and comprehensive business and risk management which provides variable compensation in the form of providing long-term revenue enhancement.

McClure (1997, p. 16) citing Toft (1997) demonstrates security's ability to generate profit through the practice of risk management, as outlined in Figure 1.

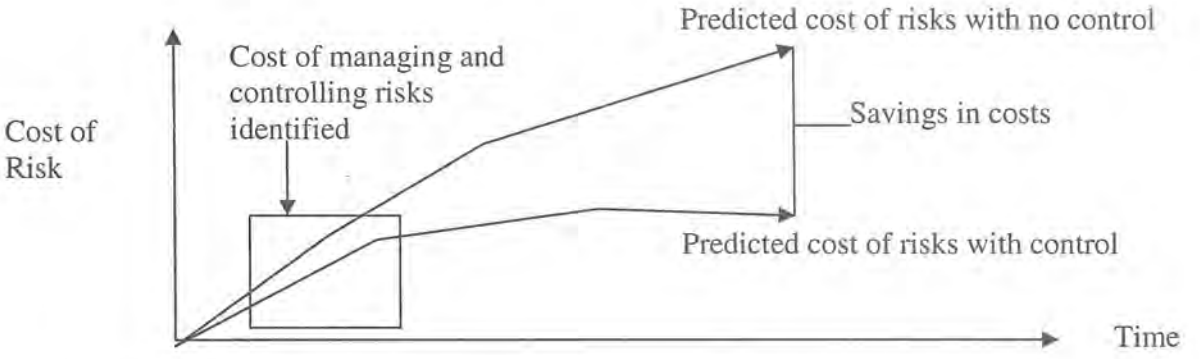


Figure 1: Risk management's ability to generate profit

In the area of board decision making, security assessments can contribute to probability forecasts which determines the probability of outcomes occurring. Risk is considered when selecting projects and choices will be dependant on the board's attitude to risk (Appleby, 1987, p. 82; Pausenberger & Nassauer, 2000, p. 272). Having access to the security discipline at the board level provides diversity in contribution and specialist skill in security risk management applied to business risk management.

In IT security, the most overlooked aspects are often the most important: passwords, training and awareness. Security and IT managers need to demonstrate to company executives how to take better advantage of the systems it already has through the use of security. There must be a champion at the board level offering senior management support in order to get things done. Often the most useful skill is how to communicate the security message in a way management and non-technical people within the company can understand and can support (Rohde, 2004).

Company reputation, uninterrupted reliability of technical infrastructures, normal business processes, protection of physical and financial assets, employee safety and shareholder confidence all rely, in some measure upon the effectiveness of an accountable, senior security function. The potential conflicting objectives among mid-level managers, often dispersing accountability, is not suitable, and can lead to a decentralised and uncoordinated security function (ASIS International, 2004).

In the context of corporate security, company officers performing in a highly competitive market, may be viewed as a corporate risk, particularly with the potential for fraud and misuse of information. Security's role on the board should be to ensure that the company has in place strategies which apply systems to appropriately monitor and detect unauthorised conduct.

> When a significant change occurs in the external environment the board must consider whether a response is required (Bosch, 1995, p. 94).

By introducing security risk management to corporate governance, the Board is recognising its accountability and responsibility to the security function. Security risk management should contribute to the reduction of risks of financial distress and failure, and upon consideration of the market, is likely to result in an improved competitive position in the company's product and labour market. This includes the interests of employees as a whole. Employees and company agents have a demonstrated interest in the success of a company, as they also incur substantial costs should the company fail. Highly skilled managerial employees make major commitments to the company and also look to continued growth of the company to provide them with rewards, in the form of promotion, status and job security (Kaen, 2000, p. 253).

Governments and regulatory agencies should support the development and functioning of risk management products and markets, like security, that assist managers and directors in carrying out their responsibilities. This support should be consistent with viewing the corporation as an institution, which promotes economic efficiency in the market place (Kaen, 2000, p. 259).

Crisis and disaster recovery planning

> ...the timely identification of risks threatening the existence of the corporation will be meaningless if the management board doesn't take adequate counteracting measures (Pausenberger & Nassauer, 2000, p. 272).

Companies will often be in conflict. Even when all parties act in good faith and with probity, conflicts and failures still occur. Honestly managed companies can fall victim of natural forces, market fluctuations and investor sentiment. Everyone honestly pursuing their self interest will create rather than eliminate conflict (Cohen & Grace, 2001, p. 101).

Crises and disasters will occur and will demand priority over routine matters. Bosch (1995, p. 105) makes the comparison between the flow of director's work with that of a war army. The army spends 99 per cent of their time waiting and training, and only 1 per cent of their time in battle, same with that of the director, as in most organisations crises occur and peaks of extraordinary pressure. Destruction of assets by fire or explosion, serious strikes, legal actions, product sabotage leading to a major product recall is likely to demand the special attention of the board (Bosch, 1995, p. 106). Crises and stresses are infrequent and their impact may be greatly reduced by preparation and planning, including the ability for directors to seek independent professional advice if necessary (Bosch, 1995, p. 121).

Following the September 11 terrorist attacks, there was an expectation that there would be a widespread move in the U.S. to centralise the corporate security function under the control of a Chief Security Officer, which would report directly to the CEO. While there was a move towards improved coordination, security management remains decentralised in most U.S. companies. There are indications of an evolution, not a revolution, in corporate security management (Cavanagh, 2004a, p. 4).

> Given the vital role played by smaller companies in the U.S. economy, the economic impact could be quite severe should we suffer another 9/11 type attack in heavily populated areas (Cavanagh, 2004b).

From all major regions in the U.S., 47 per cent of companies reported a drop in revenue following 9/11, with 80 per cent reporting disruption to business, mainly from interrupted business travel. In comparison, a major power outage in August 2003, caused 21 per cent disruption to business travel, and 13 per cent drop in revenues. This accounts for a greater severity to business from the impact of a terrorist attack. Cavanagh concludes that future assessment of corporate vulnerabilities should bear these findings in mind.

Lets suppose a terrorist attack occurs in an Australian city, and a major public company is severely affected (financially or physically) and the company has no crisis response or disaster recovery plan in place. Suppose the public and authorities become aware and choose to take recoursive action of some kind, either legally or publicly. There is a very real risk of harm to the company's reputation and financial viability if it is proven to be negligent in taking reasonable care against such a risk. However, if the company can demonstrate that it had

sufficient security risk management systems and plans in place (and therefore that any failure is not an indication of a systemic, general, fault), the company's reputation and legal standing is significantly less severely damaged as it otherwise would be (Cook, 2004).

Security risk management should comply with corporate governance guidelines in managing significant business risk, conform with Australian Standards 4360:2004 and continually monitor Australian and international case law in respect of security related incidents which have resulted in litigation or legal review. The security function integrated with corporate governance frameworks, as proposed by the *Corporate Governance Security Model*, contributes to a favourable perception of the company by demonstrating that security risk is recognised as a significant business risk and the company has risk management systems in place in the event of security events, up to and including a major terrorist attack on itself, a competitor, a client or supplier.

> The reality is that companies, regardless of size, are not immune to disruptive and dangerous attacks from many sources (Business Executives, 2004, p. 9).

A 2004 study by the Economist Intelligence Unit ("EIU") (cited by Broersma, 2004) conducted an online survey with 254 senior executives from Europe (40 per cent), the U.S. (27 per cent) and the Asia-Pacific (21 per cent) and found that 78 per cent considered security to be the top network-related issue, whilst the same number admitted to opening email attachments from unknown sources. Seventy per cent of respondents were from small and medium-sized firms and

represented the financial services, professional services, manufacturing, transportation and energy sectors.

Respondents to the EIU study indicated that 83 per cent of their attacks were initiated internally, which included sabotage, espionage and mistakes. In the previous survey, security was considered to be the second largest issue, behind reliability and availability.

The study found that security spending was moving from perimeter protection and intrusion detection to better methods for preventing attacks and recovery. 32 per cent indicated that they used or planned to use managed security services in the next two years, with 14 per cent saying they would use them in the long term. The survey found that chief executives are increasingly taking responsibility for network security policy, while some companies are beginning to appoint a chief security officer.

Benefits of Corporate Governance

> It is one thing to make non-binding guidelines available, and quite another to expect corporate entities to abide by them in the absence of rewards, incentives or some evidence that these changes will bring tangible benefits to the stakeholders of the organisation (Sarre, 2001, p. 305).

When organisations deal with a fault or issue, its proactive nature can actually enhance its reputation, not by what the problem is, but by *dealing with it* and showing that the company was *ready to deal with it* in an appropriate manner which displays integrity (Cohen & Grace, 2001, p. 110). A proactive and

innovative response to the current security environment, with its current high profile, can launch a company's credibility in its risk management, corporate governance and its potential longivity. A response of denial, inaction or indecision can have dire consequences to the reputation of the company in the market place, the directors and therefore the company value to its stakeholders.

Preparedness requires the development of company and industry specific programs and procedures. In relation to preparing for potential terrorist threats in Australia, experience in the U.S. has shown that companies of all sizes desire guidance on what constitutes a reasonable response for developing Preparedness and Response Plans (Business Executives, 2004). In most cases, the business community will not be knowledgeable about the roles, responsibilities or interactions of public health, safety, emergency and security agencies.

Making investment decisions with a lack of information, experience and under high levels of uncertainty is extremely difficult. Companies are susceptible of investing incorrect amounts, in incorrect activities or those which provide lower than optimal returns. The decision to invest in terrorism mitigation is such a decision. There is difficulty in quantifying the terrorism threat in Australia by the lack of information on the context of terrorism, identifying company risks to terrorism, analysing those risks, vulnerabilities and probabilities, and treating those risks. The decision process must evaluate the effectiveness of any counter-terrorism measure (Yates, 2003).

Yates proposes that there are few people in Australia with any experience in the complexities of terrorist action recovery and the consequence of information uncertainty in decision making is likely to result in a sub-optimal investment in critical infrastructure protection (Yates, 2003).

International terrorist attacks and the radical perpetrators present the world with a grave crisis. Rumsfeld (cited by McGeough, 2004, p. 44) asserts that terrorism is not solely a military conflict, instead it is multi-dimensional, with political and economic focus.

It is not possible to develop a generic Preparedness and Response Plan which would be effective for the diverse size, nature, location, activity and structure of business organisations. Company specific risk assessments must be conducted, with those exhibiting strong public profiles, reliance or control on critical infrastructure or known political ties identifying themselves as attractive targets for attack (Business Executives, 2004).

Corporate threats in the current international security environment can come from radical international organisations, domestic extremist groups, organised crime networks and current or past employees. Companies must plan for a variety of attacks and events, and understand the governmental framework in place to respond to each event. Other responses include addressing personnel health and safety, emotional distress and a plethora of business continuation issues (Business Executives, 2004).

The scope and scale of the U.S. and European threats of terrorism and organised crime, measured against Australia's standing indicates that Australian companies are not sufficiently prepared for a significant crisis, such as a major terrorist strike.

The costs of a crisis event in Australia can be significant. In 1998 an explosion occurred at the Longford Gas Plant in Bass Strait. As a result, oil production was reduced by $750 million, with 40% of this amount intended for the Commonwealth Government in taxes and a further $1.3 billion cost to the Victorian economy. The uncaptured costs in the event of infrastructure unavailability, or cost of accidents by infrastructure users, include losses to national economic activity, slow down of regional economic growth and decreases in national productivity (Yates, 2003).

In July 1996, the President of Daiwa Bank, Japan, received a letter from an employee confessing to fraud and embezzlement resulting in losses of US$1.1 billion. Aware that the bank had failed to supervise the employee appropriately, the board made a critical mistake. They did nothing, floundering to make a decision. After two weeks, the bank informally informed the Ministry of Finance (MOF). The MOF also kept quiet and allowed the board to continue debating on a course of action. It took three months to finally notify the MOF and the Federal Reserve. The bank was subsequently indicted in the U.S. for conspiring to hide the losses, was required to close its U.S. operations upon losing its banking licence, and paid $340 million in fines (Tschoegl, 2000, p. 109).

The leadership and experience of the board will be required in the event of a company crisis. The three obvious stages to a crisis are; before the crisis, during the crisis and after the crisis, and there is a role for the board at each stage (Hansell, 2003, p. 127).

A company should have, as a minimum, a generic response plan which can be adapted and implemented in the event of a crisis situation. The role of the board should be to review any crisis response plan developed by management (Hansell, 2003, p. 127). In the event of a crisis, one of the issues will be how the directors will discharge their responsibilities effectively. The most efficient manner will be to strike a committee to deal with or oversee the matter. Another important consideration is to ensure that the board is independent of the issue, particularly in cases where impropriety on the part of the board or senior management is concerned (Hansell, 2003, p. 129).

Following a crisis, either within the company, or related to its business or market, there should be a full post assessment and debriefing of all relevant facts. Following immediate litigation considerations, the executive and the board should openly discuss the crisis and its management effectiveness with the aim to learn from the experience. Walter (2000, p. 35) asserts that "...when a disaster occurs, everyone in the industry should know about it and be well informed on the issues involved."

A closer look at some of the major corporate disasters shows that trouble began with initial inadvertent behaviour which got worse, with subsequent efforts being to cover up the situation. The Daiwa Bank case study showed that the crisis was the result of unauthorised employee behaviour and then director behaviour. There were circumstances within the company, which allowed this to occur.

Managerial trends, which have increased the scope for fraud, according to Huntington (cited by Tschoegl, 2000, p. 113) are: matrix management, decentralisation and the encouragement of the managerial entrepreneurialism. "Of these, decentralisation and the encouragement of entrepreneurialism are most relevant to fraud and embezzlement cases."

Security culture

Boyce (cited by Eyers, 2004) asserts that the introduction of guidelines and regulations will make little difference if the corporate culture isn't right. Good corporate governance is reliant on the basic principles of acting in good faith, viewing issues from other stakeholder's point of view, and taking responsibility for actions and decisions.

Corporate culture is defined by the *Criminal Code Act 1995* (Cth) in section 12.3(6) as an: "...attitude, policy, rule, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant activities take place." Trompenaars (cited by Quirke, 1996, p. 108)

defines culture as "...a shared system of meanings. It dictates what we pay attention to, how we act, and what we value." Nadler (2004, p. 14) suggests culture is "...a system of informal, unwritten, yet powerful norms derived from shared values that influence behaviour".

A company with a poor corporate culture may be considered culpable under the *Criminal Code Act 1995* (Cth), as well as, the individual directors. According to Sarre (2001, p. 310) the legislation was designed for situations which, contrary to the existence of documentation appearing to require compliance, the reality was that non-compliance was expected. An example may include reckless endangerment where the corporate culture inferred authorised breaches of safety codes to increase productivity, despite documented safety procedures.

Organisational culture influences how people listen to company communications, such as an acute sensitivity to business speak, and a suspicion that it betrays old values. Quirke (1996, p. 14) asserts that "culture reflects communication". The company must know how their employee's listen, you may say one thing, but people hear another. Any security and risk communication must consider the methods most suited to the organisational culture of the subject company.

> Most companies are not in control of their culture; their culture is in control of them (Quirke, 1996, p. 16).

Cohen and Grace (2001, p. 113) assert that the company CEO and the board must be convinced of the benefits, of any kind, to commit to a type of organisational culture. In terms of implementing security into corporate

governance, whatever the reasons, the message from the top down must be that the company wants to develop and maintain a security culture. If the message is that the company recognises its need to develop security functions, security behaviour and a sound security environment, and if the message is serious and sincere, then those things themselves become the focus for the conduct of organisational matters.

Mcartney (cited by Fitzgerald, 2004) asserts that most employees don't consider security their responsibility, citing that the company has a security department. They have the mentality that security is someone else's problem, not theirs. Mcartney considers security to be comparable with quality assurance in the 1980's; "Like quality, these virtues are either [ingrained] in an organization or they're not. You can't put up a sign and create them."

What has become vital to manage any organisation is the ability to foster and facilitate communication within it. As the effectiveness of 'formal controls' diminishes, and the importance of line power decreases, the importance of managing the culture as a means of keeping the organisation secure and on course is paramount, and contributes added value to stakeholders, long term revenue and company longevity (Quirke, 1996).

> To be most effective, risk management should become part of the organisation's culture (AS/NZS 4360:1999).

Senior management commitment is the single most important factor in the success or failure of any risk management program, and sets the style to the toleration of imprudent or unsupervised risk-taking. There also needs to be an overarching corporate culture which leads to the issue of behavior modification techniques (Hayes & Truscott, 2004, p. 37; Walter, 2000, p. 25; ASIS International, 2004, p. 5).

Wartofsky (cited by McClure, 1997, p. 18) argues that cultural surroundings will influence people's perception of risk, and to see risk in a certain manner. Cultural influences come from values which are "socially constituted, socially learned and socially enforced." A corporate culture may be one where the need to comply with security policy and practices is non-existent. A weak security culture will influence the degree of apathy towards the provision and practice of security.

Security decay theory is concerned with the effect of security on the behaviour on personnel. The theory proposes that apathy is a result of effective security preventing threat occurrence. In McClure's (1997) study into security decay theory, the implementation of protection on risk analysis results may, if the level of protection is higher than needed, cause an over emphasis on security which will cause security to be seen as unnecessary. This results in security decay, where security measures are in place, but they are no longer operating to their intended level of effectiveness.

There is a delicate balance needed between the minimal and maximum security countermeasures. McClure (1997, p. 20) asserts that "Too little security may result in high risk materialisation, while too much security may result in decay leading to risk materialisation."

The ACCC (cited by Cohen & Grace, 2001, p. 105) has stated that strong compliance programs, such as ethical requirements and culture, do lead to a competitive advantage and value to shareholders. Quality characteristics of a company can enhance marketing and give positive return to bottom-line benefits.

Kuada and Gullestrup's (1998, p. 27) study into the cultural context of corporate governance showed that culture impacts on governance and accountability, and apart from macrocultural influences, each company develops its own organisational culture.

An effective security function is reliant on an integrating organisational structure and culture. Where the security function resides in an organisation will determine its authority and power base, and in turn its ability to contribute to strategic policy and influence decision makers. The culture of the organisation is just as important. The strength of the security culture will impact on the affect of the security function (Blades & McClure, 2003, p. 68).

Governance reform should be viewed as a catalyst for boards to change their cultures. When directors begin to develop cultures which promote candor and a willingness to challenge, they will reflect the social and work dynamics of a high performance team. As the board and management begin to start performing as a team, the organisational culture will change. Nadler (2004, p. 14) asserts that "The closer directors get to an engaged culture, the closer they are to being the best boards possible."

McKnight (cited by Fitzgerald, 2004) proposed that company cultures are hard to change but that they can become more security-conscious — "though only if top management leads the way." He asserts that companies must give attention to four areas: user awareness, physical security, new and old technologies, and policy. Companies should have a mandatory security awareness program for all employees, including the CEO. As an example, corporate security policies can protect vital information assets by way of discouraging employees from putting data on any devices that leave the borders of the physical corporate building.

Managing the corporate culture is increasingly crucial from a security perspective, as the very nature of corporate security is changing in response to significant business risks. Increasingly, the "inner-market", incorporating those working in and comprising the company, become 'knowledge workers' and independent professionals, whose behavior cannot be directly monitored or evaluated (Quirke, 1996, p.15). This creates a security risk and is a challenge for

the board to control. Quirke (1996, p. 15) asserts that "hierarchical power can no longer be relied on to deliver dictates from the top."

A study by Gurdon (2001) into new employee socialisation and the security function proposes that companies should have a socialisation and security framework, which incorporates practices to encourage and reinforce security related positive behaviour. From a security prospective, behavioural standards should promote and maintain a security conscious and ethical culture, which reflects the organisation's nature and industry affiliation.

Gurdon (2001, p. 106) proposes that "Motivating employees to be vigilant and supportive of security activities will be difficult to achieve without positive reinforcement...the security function must, at a minimum, support behavioural standards, the reporting of dishonest activity, and adherence to policy and procedures."

Positive reinforcement, through recognition and awards, should have the support of management and the board. Top level support will establish the legitimacy of the socialisation and security association. Informal reinforcers, such as feedback, should be diligently applied to prevent security decay. Punishment and negative reinforcement should be applied to undesirable or 'security risk' behaviour. Guidelines should exist which detail how punishment is to be applied. During any disciplinary process, the cultural influence of the workgroup should also be

examined, and behavioural standards and security-based training altered if required (Gurdon, 2001, p. 108).

Codes of Conduct

Australian organisations, following the lead from the U.S., have adopted codes as part of the reform of business culture. Farnham (cited in Cohen & Grace, 2001, p. 120) showed in his study into codes that while they are not as frequently or appropriately used by employees as would be desired, nevertheless they are significant in changing behaviour in corporations.

Codes are well adapted to the needs of corporations, as they are not natural persons but a legal entity which has a culture, but no character, conscience or emotional life. Codes of conduct are a way of setting standards and guiding conduct (Cohen & Grace, 2001, p. 121; Dang, 2000, p. 16; Bosch, 1995, p. 187). Security addressed in the code of conduct will not take the place of other security measures, but the fact that they cannot do everything does not mean that they are useless.

The production and implementation of a code is the directors and manager's responsibility. Cohen and Grace (2001, p. 122) assert than unless the culture has been subject to an audit and declared safe, it is a risk to use any other standard to which the provisions of the code can be measured. Codes should be 'rolled out', rather than just posted and appeal to the probity of all company members.

Cohen and Grace (2001, p. 122) discuss 'institutionalising ethics in corporations' and offer nine schematic guidelines. Leadership is considered the most important factor in staff compliance with corporate norms, and creating and sustaining an organisational culture. Applying these guidelines to enhancing a security culture, the schematic guidelines proposed are;

1. The board of directors and management must be publicly committed to security in actions and words. Hypocrisy must be avoided by those responsible for managing a corporation (Cohen & Grace, 2001, p. 22; Walter, 2000, p. 34). Commitment is shown by including security policy in corporate governance statements ;
2. Policies and procedures are developed for addressing security issues and events which may impact on business activities;
3. Security functions are included in the corporate code of conduct, regularly considered in decision making and training is provided. While these are tangible signs of security awareness, they are not recognised as standalone security measures;
4. Adequate security advice, either internal or external, is available to field security questions, monitor compliance with security procedures and to recommend revision of the code and policies;
5. Security training programs form a regular part of staff development and induction;
6. Sound security behaviour is rewarded and never punished for not producing results;
7. Insecure behaviour is not rewarded even if it gets bottom line results;

8. Employees should not be exposed to avoidable security situations that put them at risk and should be provided with secure work environments; and
9. Individuals should be encouraged to discuss security concerns with supervisors and report misconduct via credible whistleblower and reporting systems.

Communicating security

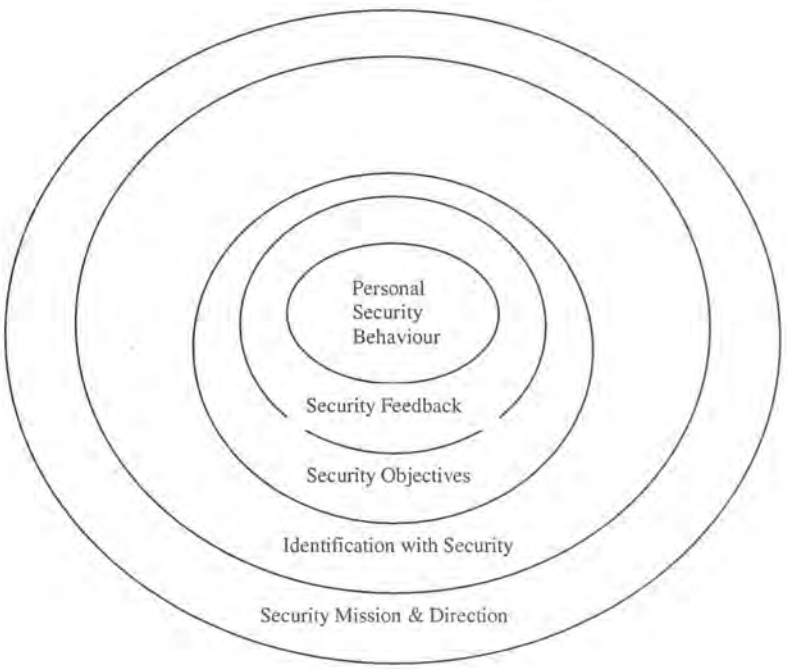
In changing or introducing a security culture, the role of communication should be to create awareness that the security problem the organisation faces has changed, in the face of the inclination to avoid the harsh reality. Changes in culture occur when people realise that the old ways of doing things are only suitable to an environment which has passed. It is easier to change the organisation when the people share an understanding of the security situation they face, the inappropriateness of old behaviour and the need to find new solutions (Quirke, 1996, p. 109).

To achieve the best results security needs to be humanised, as has been done with safety. In the absence of strategic information, every employee must watch out for and actively report suspicious activity. It is essential that there is a system of collecting security related information as intelligence. This is the only chance to obtain an early warning against a terrorist or security related attack. The reality is that government or police agencies are seldom able to deliver early warning of any specific value for the protection of business facilities (Hayes & Truscott, 2004, p. 37).

Applying the levels of communication, proposed by Quirke (1996, p. 26) to corporate security awareness, in order to be successful, people need firstly to have a sense of belonging to the company and a sense of pride in what the business does. They need to be informed about its activities and clear about its direction. There needs to be trust in management and confidence in leadership. To create a security culture in this environment, the company's people;

1. Need to understand the overall security vision, mission and direction;
2. Need to feel part of the security solution and understand their responsibilities;
3. Need to know the company's security objectives and how they relate to them;
4. Need to understand, be clear about and get feedback on security issues and incidents; and
5. Need to understand and get feedback on their own security behaviour.

Figure 2; Levels of security communication



"Credibility is a strategic resource. It takes a long time to build, and an extraordinary short time to lose (Quirke, 1996, p. 100)." Like crisis communication, there is growing sensitivity to the impact a security incident can have on a business, and security communication will need to be a discipline enforced to protect the credibility of the company and its brands. Corporate reputation may withstand a very small degree of damage from time to time, but damage greater than that can be extremely costly to company stakeholders (Walter, 2000, p. 33).

The role of security communication is not primarily the 'top-down' dissemination of management thinking, but the 'bottom-up' means of connecting those who are security aware and who know what needs to be improved, to those who have the authority to make changes happen.

Communicating the company's quality characteristics in the form of corporate governance disclosure can lead to a competitive advantage and be attractive to shareholders. A company implementing comprehensive security policies and developing a sound security culture to protect itself and its long term interests in the wake of terrorism and corporate threats, communicates to stakeholders that the board has seriously considered the potential threats of the international security environment and the potential impact on the company. In response the board has enhanced its security culture, and accepts its continued responsibility to the company's strategic security in its corporate governance.

CHAPTER 3

The Study

Study Procedure

This study aimed to determine the degree of recognition and application of the security risk management function to corporate governance practices in Australia. Formal research design used descriptive research methodology, consisting of a literature review, primary document analysis and a questionnaire survey to collect data. This research was contrasted to a formulated *Corporate Governance Security Model* to determine if the model is applicable to the recognition, or application, of security to the ASX Corporate Governance principles.

The procedure for the study consisted of the following 6 stages;

1. Development and Pilot Study;
2. Literature Review, Document examination and data collection;
3. Respondent contact and questionnaire completion;
4. Data Analysis and statistical calculations;
5. Comparative review of Model; and
6. Recommendations and Conclusions.

Design

The literature review involved a comparative study of company theory, director duties and responsibilities, corporate governance and security management literature and practices. This defined corporate governance, identified how effective corporate governance is achieved and its ability to create value and competitive advantage. The review examined the roles of the board, corporate governance practices, security risk management in corporate governance, case studies and an analysis of applications of security in treating significant business risks and emerging security risks.

Document analysis and subsequent data collection consisted of locating disclosure of the subject's security function and its relationship with the subject's corporate governance practices. Corporate governance disclosures by the target population were accessed with subjects having websites where their documents were readily available.

The analysis involved identifying the subject's current corporate governance framework from public documents released in the form of Annual Reports, Corporate Governance Statements, Policy and Principle Statements. These publications were reviewed to determine what risks they highlighted as forming part of their internal controls, risk management and corporate governance. Primarily, the major areas selected for further analysis were environmental

policy, health and safety policy, risk management policy, asset protection, reporting policy and security policy.

A questionnaire survey of the target population was designed to determine the company's recognition of security in its corporate governance practices. A website was designed and posted online to explain the purpose and significance of the study and allow respondents to complete a questionnaire on line. Respondent companies were emailed and telephoned to request their participation and invited to visit the research website. Respondents then completed the questionnaire on-line and responses were automatically emailed direct to the researcher. Responses were then transferred to a spreadsheet to accommodate the data analysis.

A corporate governance model was formulated to identify security's risk management role in each of the ASX Corporate Governance Principles (2003). This provided a subjective outline of where security may be recognised and where it has an applied function within the corporate governance framework. The model endeavors to provide a framework and allow a comparison to be made between how security risk management can be applied, and how security risk management is currently applied.

Samples and Subject Selection

In 1994 there were approximately 1100 companies listed on the ASX (Bosch, 1995, p. 3), and this had grown to 1500 in 2004 (Dobbie, 2004, p. 25). Most of the companies are small, yet, as Bosch (1995, p. 3) asserts "the economic importance of the top 200, the size of the capital invested in them, the numbers of people they employ, the general familiarity with their products and services, and such is the fear of the damage they could do that, to most people, they characterize modern capitalism."

Applying this assertion to this study, randomly selecting 60 of the ASX/S&P 200 companies provides a sound indication of corporate security management following the emergence of the 'War on Terror' and the companies most likely to be either targeted, or affected, by any terrorist attack on critical infrastructure in Australia.

The target population was therefore the top 200 publicly listed companies on the ASX All Ordinaries Index. This allowed for a population frame and restricted the study to medium to large organisations. Random selection of 60 companies listed on the ASX/S&P 200 as of 1 May 2004 formed a subset population, representing a 30 per cent sample size.

Of the sixty companies selected, respondents to a questionnaire were sought by stratified random sampling (Sekaran, 1992, p. 231) by identifying non executive directors and executive managers who were members of an audit, or appointed, committee which related to corporate governance. The selected respondent's email was sought from the company's website, annual report or direct inquiry to the company.

Document analysis

Data collection procedures from document analysis involved the examination of company websites and their compliance to corporate governance guidelines in the form of disclosures in their Annual Report, Corporate Governance Statements, Policy Statements, and Statements of Principles. The company's corporate governance statements were analysed to identify any recognition or application of a security risk management function.

Data from document analysis was used to determine the company's core business and activities (sector), medium and long term strategies, corporate policies, and corporate governance practices. This data determined the company's exposure and involvement to security related issues and the current security environment.

Data collection recorded if the company had an audit committee and a risk management committee. Within the corporate governance statement and the disclosed role of the audit and risk management committees, it was recorded if the company recognised environmental risks, occupational health and safety

risks, asset protection policy, an incident reporting policy, and any other specific security function.

Statistical calculations were performed within the response's spreadsheet which determined the percentage of the target population complying with corporate governance guidelines and the recognition of a variety of risks, including security risks. Sixty medium to large public companies were randomly selected from the sample size of two hundred, and their company announcements and reports were analysed.

Statistical calculations were finalised to determine the frequency and degree to which security is applied and how it was integrated to enhance the company's current corporate governance practices. If the *Corporate Governance Security Model* is an appropriate concept, the data should support and justify the research questions.

Research instruments

Questionnaire

The aim of the questionnaire was to determine security's current function in corporate governance and if the changing security environment is encouraging its application in the field of risk management.

Questionnaires, unlike psychological tests and inventories, have a very limited purpose. They are often one-shot data gathering devices with a very short life, administered to a limited population (Best, 1981, p. 179).

A generic email was created to communicate the study's significance and proposed role of security in enhancing corporate governance. In the email respondents were directed to the research website to complete the questionnaire on-line in the form of structured questions.

Targeted sampling was used where the respondents were selected based on selection criteria set out below. The use of email communication allowed for a greater sampling size to be obtained but reduced the number of responses due to company email policies and a lack of direct communication with the researcher. The number of respondents completing the questionnaire has provided a very limited view of board level security management practices.

The correct sample size depends upon the purpose of the study and the nature of the population under scrutiny. A sample size of thirty is held by many to be the minimum number of cases if there are plans to use some form of statistical analysis of the data (Cohen & Manion, 1980, p. 77). This study targeted sixty respondents.

The questionnaire consisted of a closed form type. Closed form calls for short, check responses (Best, 1981, p. 169). Responses were either yes, no, not known or decline to answer.

Consideration to the characteristics of a good questionnaire included that it;

- ✍ Deals with a specific topic which will be recognised as important enough to warrant the respondents time in completing;
- ✍ Seeks information which can not be obtained from other sources;
- ✍ Short as possible;
- ✍ Attractive in appearance;
- ✍ Directions are clear and complete with all terms defined and questions worded simply;
- ✍ Questions are objective with no leading questions;
- ✍ Questions are presented in proper psychological order, proceeding from general to more specific responses; and
- ✍ It is easy to tabulate and interpret.

(Best, 1981, p. 176)

Questionnaire data was analysed to determine the respondent's;

- recognition of an existing security function in corporate governance;
- recognition of security management qualifications or experience;
- response to changes in security environment; and
- acknowledgment of a security function in corporate governance practices.

Corporate Governance Security Model

In conducting data analysis, the objective was to measure the frequency and degree in which the *Corporate Governance Security Model*, as attached at Annexure 3, would be expected to enhance a company's corporate governance and risk management practices.

Applying the data collected to the developed model, the degree and frequency of contribution security risk management can make, was compared to the applications security has or would be expected to have in the company's corporate governance practices.

The frequency and degree of security management applications in corporate governance will provide support to the research questions, and an indication as to whether the security model can be effectively applied and then enhance corporate governance practices.

Pilot Study

The generic email, as attached at Annexure 1, was sent to three independent people who matched the criteria as being involved in executive company management. The email directed the pilot respondents to the questionnaire for participation, as attached at Annexure 2.

The three pilot respondents completed the questionnaire without difficulty and did not raise any issue with the process or question structure. One suggested significantly expanding the questionnaire and to include a Likert scale, however adopting the suggestion would have been outside the scope and capability of the study.

The pilot study identified the subjective nature of the research and the likely impact of respondent positions as senior company executives and board directors. These included restricted time commitments, scope of other issues they must contend with, and the general perception that they do not imminently face significant security related risks.

Ethical Considerations

The target population in this study is publicly listed companies on the Australian Stock Exchange. The participants in the questionnaire were representatives of the company, and therefore the study involved human participation.

Ethical considerations of peoples consent and confidentiality was properly considered and protected in accordance with ECU Policies and Procedures in the conduct of ethical research involving human subjects (ECU Policies and Procedures, 2005).

Limitations

This study had a number of limitations arising from the research design. The most significant limitation identified prior to the study was to overcome a foreseen lack of company director participation and to communicate the significance of the study.

The major limitation was promoting the study to a level which demanded participation, such as seen in existing studies such as the *Computer Crime and Security Survey*, conducted annually. This study was titled the '*National Corporate Governance and Security Survey*' and listed on an ECU Website to raise the profile of the study. This had little perceived impact on increasing responses. This resulted in a limited acknowledgement and participation by the sample population.

A low response of only ten per cent was received to the questionnaire. The initial target company representatives sought to participate were Company Directors. During the study's proposal Company Directors were identified as a potential limitation. As foreseen, Company Directors were very difficult to communicate with directly, either by phone or email. Some responses declined to participate stating that their directors were simply too busy.

It may be suggested that public companies either did not find the study significant enough, have a generic, yet convenient, policy of not disclosing or discussing their security, do not regard security as an important issue or are reluctant in giving security any recognition at the board level of the company.

Limitations also exist with the accuracy of the responses. As the study proceeded with little response, a second round of approaches was made to the target population which sought company representatives at the senior management level responsible for either security or corporate services. This level of management may be unaware of what their board's responsibilities are and may have made assumptions concerning questionnaire responses.

While the characteristic of these limitations may impact on a study of this kind, particularly in drawing questionnaire responses, it is suggested that they have been further exasperated by a poor recognition of security within the current corporate governance framework.

Chapter 4

Study Results

This chapter introduces the data collected from the document analysis and the questionnaire responses. Statistical calculations are presented in graphical format to allow immediate and clear assessment of their relevance to the research questions.

Document Analysis Results

The sixty companies randomly selected from the ASX 200 represented a broad range of private sectors, as per Annexure 4. Nineteen (19) different private sectors are represented. The two sectors with the greatest representation are Materials (31%) and Energy (10%).

Table 1 presents the document types examined. A majority of public companies selected had annual reports and corporate governance statements accessible from their website. Only one subject in the population did not provide documents online and one provided a Statement of Principles. Table 2 and Figure 3 present a break down of the different sectors represented in the target population.

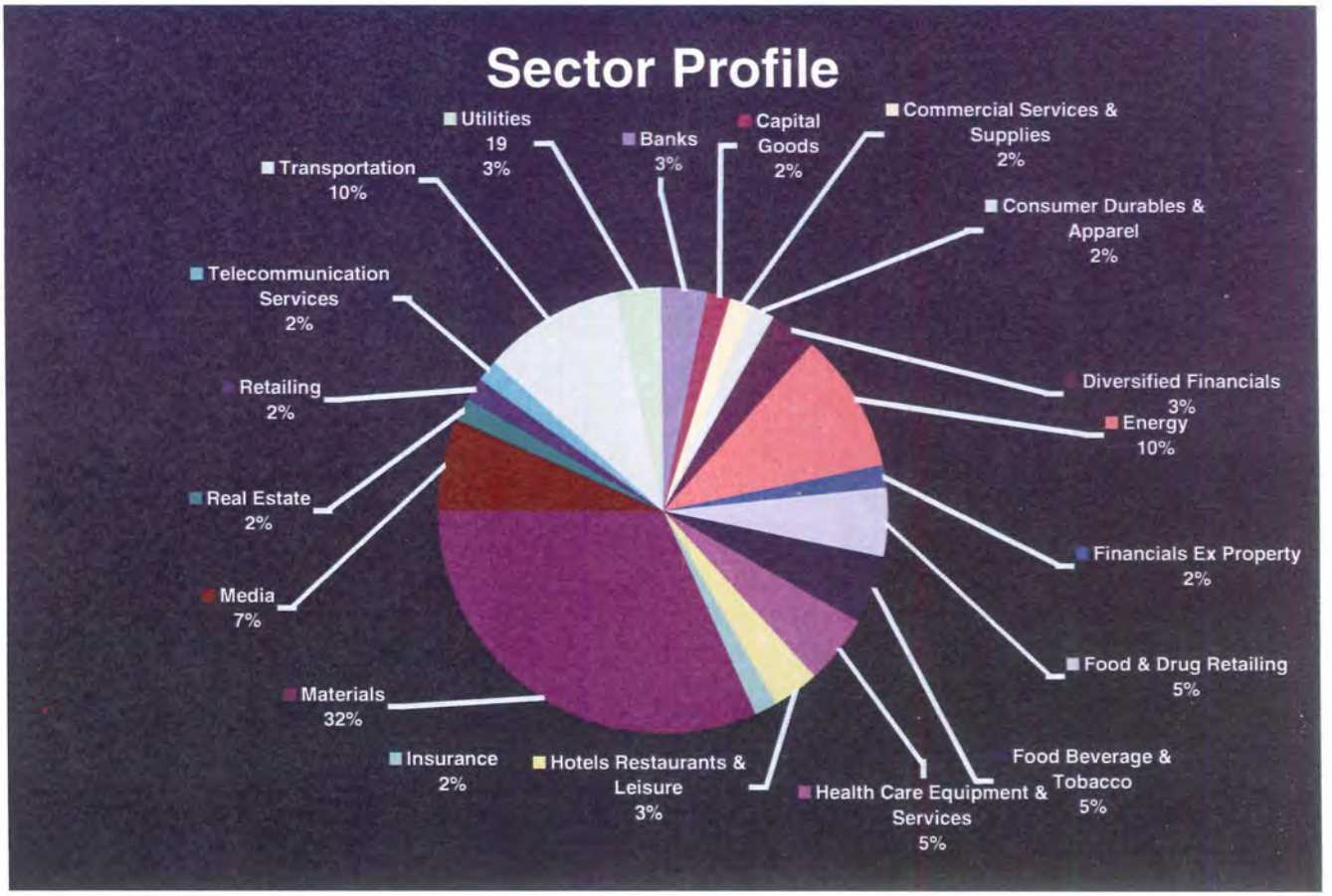
Table 1. Document Types examined

Document Type	
Annual Reports	27
Corporate Governance Statements	31
Statement of Principles	1
No online information	1
TOTAL	60

Table 2. Sector Profile of Target Population

Sector Profile		
	No.	Percentage
Banks	2	3.33%
Capital Goods	1	1.66%
Commercial Services & Supplies	1	1.66%
Consumer Durables & Apparel	1	1.66%
Diversified Financials	2	3.33%
Energy	6	10.00%
Financials Ex Property	1	1.66%
Food & Drug Retailing	3	5.00%
Food Beverage & Tobacco	3	5.00%
Health Care Equipment & Services	3	5.00%
Hotels Restaurants & Leisure	2	3.33%
Insurance	1	1.66%
Materials	19	31.66%
Media	4	6.66%
Real Estate	1	1.66%
Retailing	1	1.66%
Telecommunication Services	1	1.66%
Transportation	6	10.00%
Utilities	2	3.33%
TOTAL	60	100%

Figure 3. Sector Profile of Target Population

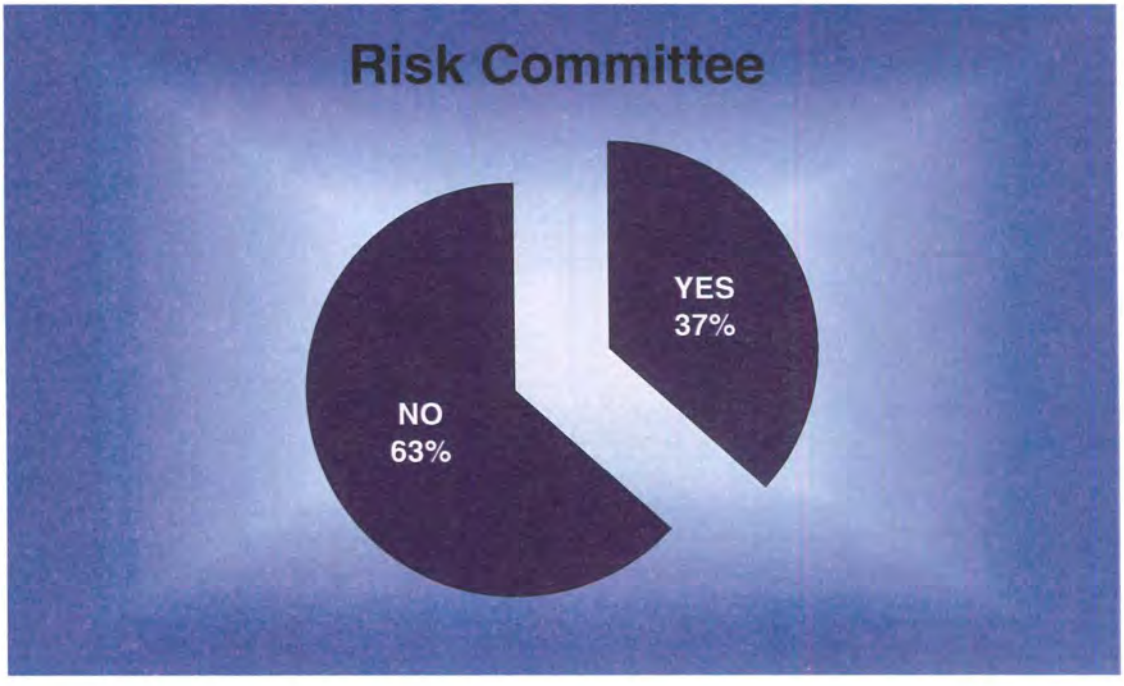


Statistical Calculations from Document Analysis

Audit and Risk Management Committees

Only one company in the target population was found not to disclose the existence of an audit committee on their website, otherwise all companies in the target population had an audit committee. Only 37 per cent of the target population disclosed having a risk management committee as depicted in Figure 4.

Figure 4. Target Population's disclosure of a Risk Management Committee



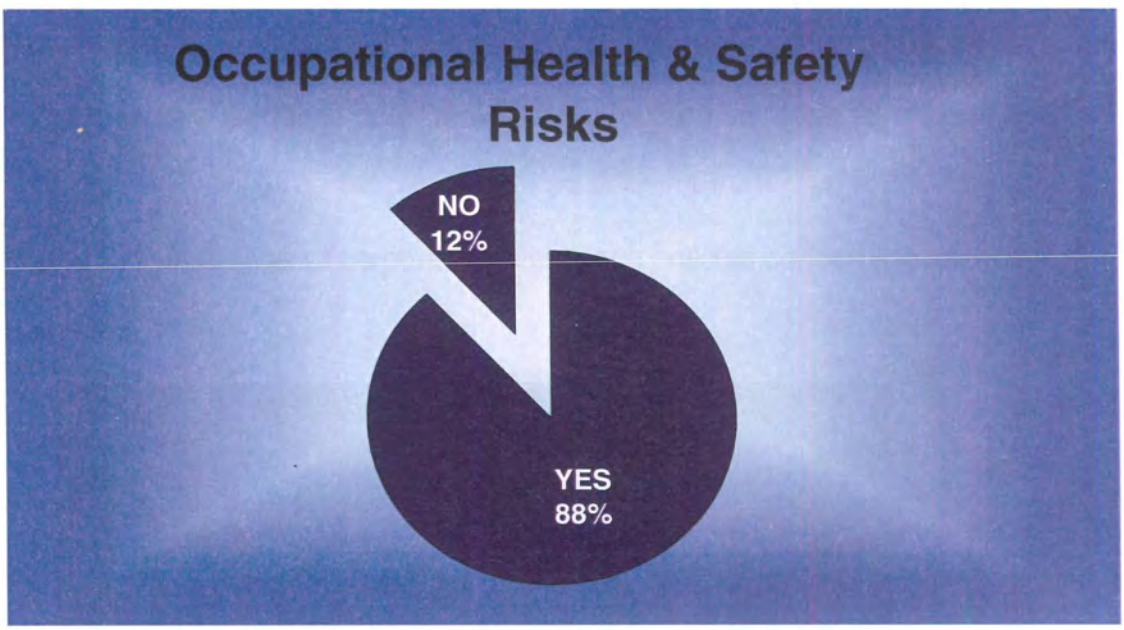
Environmental and Occupational Health and Safety Risks

More than 85 per cent of the target population disclosed corporate governance practices relating to their environmental risks and occupational health and safety risks. Disclosure varied between detailed policy and practices statements to thorough to generic commentary in annual reports.

This demonstrates that environmental and occupational health and safety is widely integrated with corporate governance and risk management for ASX listed companies. Demonstrating and publishing such compliance in corporate disclosures may be seen as adding value to the company's reputation.

Figure 5. Percentage of corporate governance policies concerning environmental risk.

Figure 6. Percentage of corporate governance policies concerning occupational health and safety risk.



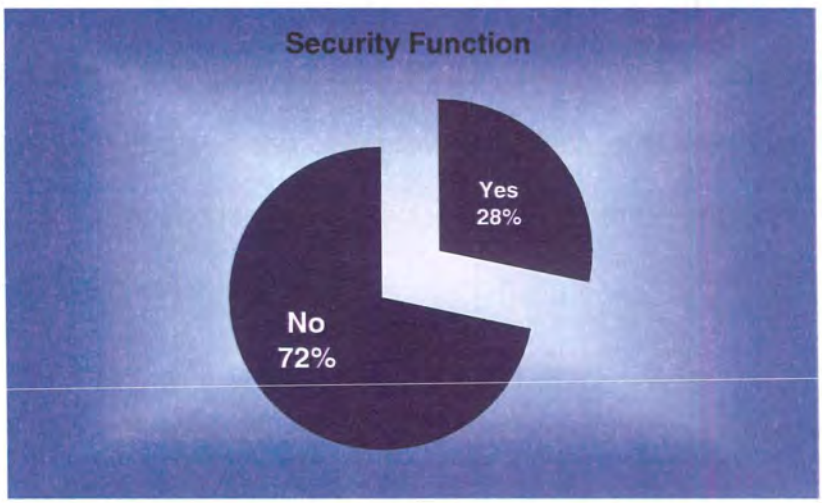
Asset Protection and Security Risks

Less than 30 per cent of the target population disclosed corporate governance practices relating to their asset protection or security related risks. Many security related disclosures which were made were found to lack any substance, with only two companies in critical industry sectors (Telecommunications and Transport) having detailed security policies integrated into their corporate governance framework.

These findings indicate that there is a significant lack of recognition in relation to security risk management and asset protection policies. Compliance in the functions of security and asset protection is not mandatory and therefore may be given less attention as a result, particularly when compared with environmental and occupational health and safety legislation, and therefore compliance requirements in these areas. There may be substantial scope for the Corporate Governance Security Model to contribute to corporate security risk management in the form of a guidance note or regulatory recommendation for compliance.

Figure 7. Percentage of corporate governance policies concerning asset protection.

Figure 8. Percentage of corporate governance policies concerning a security function.



Reporting Policy

Less than 40 per cent of the target population disclosed corporate governance practices relating to any reporting policy. Many reported disclosures were only briefly noted under occupational health and safety policies.

Figure 9. Percentage of corporate governance policies concerning reporting policy.

Questionnaire results

Due to the poor response (10 per cent) to the approach email, as attached at Annexure 1 and the questionnaire, as attached at Annexure 2, the sector profile is extremely limited and can only provide an individual response to represent an entire sector. Subsequently the sector profile of the questionnaire respondents contributed little value to the study.

Table 3. Sector Profile of Target Population completing questionnaire

Sector Profile		
	No.	Percentage
Materials	3	50%
Health Care Equipment & Services	1	16.66%
Media	1	16.66%
Food & Drug Retailing	1	16.66%
TOTAL	6	100%

Statistical Calculations from Questionnaire

The questionnaire consisted of 19 questions which sought responses to determine the following;

Part 1 Recognition of an existing security function in Corporate Governance;

Part 2 Recognition of security management qualifications or experience;

Part 3 Response to changes in security environment; and

Part 4 Acknowledgment of applied security functions in corporate governance practices

Part one of the questionnaire sought to determine the current recognition of the security function by the board of directors in the corporate governance framework. Only a third of respondents documented security functions as a board responsibility. Half documented security functions as an audit committee responsibility.

All respondents included security management in its review of internal controls. Half stated they integrated security policy with corporate governance policy. A majority of the respondents had a policy promoting a security culture. Table 4 outlines responses to Part 1. This demonstrates that security functions are recognised by respondents but security is not isolated in policy statements and risk management practices. Implementing the corporate governance security model would provide guidance to companies recognise their existing security functions allow for security policy formulation.

Table 4. Responses to Questionnaire Part 1.

Part 1 Current recognition of the security function

Respondent	Security documented as a board responsibility?	Security documented as an audit committee responsibility?	Security in review of internal controls?	Integrate security policy with corporate governance policy?	Policy promoting a security culture?
Materials	No	No	Yes	No	No
Materials	No	No	Yes	No	Not known
Materials	Yes	Yes	Yes	Yes	Yes
Food & Drug Retailing	No	Yes	Yes	No	Yes
Media	Yes	Yes	Yes	Yes	Yes
Health Equipment & Services	No	No	Yes	Yes	Yes

Part 2 of the questionnaire sought to determine the recognition of security management qualifications and experience on the Board of Directors. No respondent company had a member of the board with any qualifications or experience in security management. Only a third of respondents had a member of the board or committee with designated responsibility for the security function. Five of the six respondents had sought external security advice in the previous two years, all respondents considered that corporate security advice was available and a majority stated they would consider obtaining independent security advice, with one respondent answering not known. Table 5 outlines responses to Part 2. These results provide that companies are willing to seek out and listen to security related advice, giving credence to a potential need for a model by which security can be consistently implemented into corporate governance practices.

Table 5. Responses to Questionnaire Part 2.

Part 2 Recognition of security management qualifications and experience on the Board of Directors

Respondent	Board or senior executive has qualifications or demonstrated experience in security management?	Board or an appointed committee has designated responsibility for security management?	Board or an appointed committee sought external advice regarding a security related issue within the last 2 years?	Considers that corporate security advice is available?	Considers obtaining independent security advice?
Materials	Not known	No	Yes	Yes	Yes
Materials	No	No	Yes	Yes	Yes
Materials	No	Yes	Yes	Yes	Yes
Food & Drug Retailing	No	No	Yes	Yes	Yes
Media	No	Yes	Yes	Yes	Yes
Health Equipment & Services	No	No	No	Yes	Not known

Part 3 of the questionnaire sought to determine a response to perceived changes in the security environment. A majority of respondents had recognised changes in the security environment over the last five years which have increased their business risks. Half considered that the current security environment presents significant business risks to the company. Only a third had reviewed security policy or audited security procedures in the previous two years, although two thirds had informed their board or appointed committee of an internal security event or incident in the previous 12 months. Table 6 outlines responses to Part 3. The interest of directors and board committees in security related internal controls provides an opportunity for the *Corporate Governance Security Model* to provide a mechanism by which security is nominated as an agenda item which is regularly reviewed and discussed at the board level.

Table 6. Responses to Questionnaire Part 3.

Part 3 Response to changes in security environment					
Respondent	Recognised changes in the security environment which have increased your business risk within the last 5 years?	Consider that the current security environment presents significant business risks to your company?	Board or an appointed committee reviewed security policy within the last 2 years?	Board or an appointed committee audited security procedure within the last 2 years?	Board or an appointed committee been informed of an internal security event or incident in the last 12 months?
Materials	No	No	No	No	No
Materials	Not known	No	No	No	No
Materials	Yes	Yes	Yes	Yes	Yes
Food & Drug Retailing	Yes	Yes	Yes	Yes	Yes
Media	Yes	No	No	No	Yes
Health Equipment & Services	Yes	Yes	No	No	Yes

Part 4 of the questionnaire sought to determine if a security function would be acknowledged if applied to corporate governance practices. A majority of respondents regarded good security practices to form part of good corporate governance and would consider that corporate governance is, or would be enhanced by the application of a security function. Only a third of respondents considered that the application of a security function to corporate governance would contribute to long term revenue enhancement of the company. A majority considered that company stakeholders would favour disclosure of a security function within corporate governance disclosures. Table 7 outlines responses to Part 4.

Table 7. Responses to Questionnaire Part 4.

Part 4 Acknowledgment of applied security functions in corporate governance practices

Respondent	Regard good security practices as part of good corporate governance?	Consider that corporate governance is, or would be, enhanced by the application of a security function?	Consider that an application of a security function to corporate governance contributes to long term revenue enhancement?	Consider that company stakeholders would favour disclosure of a security function within corporate governance disclosures?
Materials	Not known	Not known	Not known	Not known
Materials	Yes	No	No	No
Materials	Yes	Yes	Decline to answer	Yes
Food & Drug Retailing	Yes	Yes	Yes	Yes
Media	Yes	Yes	No	Yes
Health Equipment & Services	Yes	Yes	Yes	Yes

Chapter 5

Data Analysis and interpretations

Analysis of the study results was conducted to determine any common themes or interpretations in the recognition and awareness of security risk management in corporate governance practices in the target population.

The analysis of the percentage calculations from the 60 companies randomly selected from the ASX 200 and their disclosed corporate governance statements strongly suggest that security related risks are not widely recognised or considered as part of the corporate governance framework.

Therefore, in answer to research question one, the *Corporate Governance Security Model* does not recognise an existing security function in current corporate governance practices.

85 per cent of companies disclosed environmental and occupational health and safety risks which are given due attention and are well documented in annual reports and corporate governance statements. However only 28 per cent documented any asset protection or security related responsibilities. This included analysis of risk management committee charters, in which security risks were often not raised as part of the risk management context. Only 38 per cent documented any reporting policy suggesting many companies do not have

procedures in place concerning the reporting, recording and analysis of security related incidents. Companies are therefore unlikely to be aware of the real cost of security, the return on investment they receive from security spending, and trends which may be leading to inherent, but preventable losses.

Analysis of questionnaire results identified that a majority of company boards do not have a documented responsibility for a security function and directors are unlikely to have any demonstrated experience or qualifications in security management. Questionnaire respondents indicated that security was reviewed as part of internal controls and that security was integrated into corporate governance policy.

Comparison of the respondents' questionnaire results and document analysis suggests that although companies may have a security function operating, it is not disclosed in corporate governance statements or other publications. There is limited substance to the claim that companies consider the existence of internal security controls confidential. Company stakeholders have an interest in knowing that the company they associate with recognises and is managing their security responsibilities and risks.

Application of data analysis to Corporate Governance Security Model

Currently, a majority of Boards in Australian public companies have not documented their responsibility or recognition of security risk management within their governance framework. This is in contrast to the model which proposes that security functions be incorporated as a responsibility of the board under Principle 1 and included in the Board's charter.

A majority of questionnaire respondents cited independent security advice to be available and utilised by company boards. This is consistent with the model in Principle 2, recommending Boards' add value by having procedures in place to take independent professional advice if necessary. The model proposes the board recognise security management as a profession and seek information and specialist advice on security issues when necessary.

With limited application of security risk management in the corporate governance framework, there is less focus on security related behaviour within the codes of conduct held by a majority of public companies. Although a majority of questionnaire respondents indicated they incorporated a policy promoting a security culture, there was no evidence found in the company's public documents advising stakeholders. The model at Principle 3 and Principle 10 proposes the implementation of security awareness within the Code of Conduct to highlight the responsibility on all company officers and employees to promote awareness and

recognition of protecting company assets and mitigating loss from security related breaches.

All respondents included security functions in its review of internal controls and this is consistent with supporting literature research. Audit committees and risk management committee's are certainly inclined to examine obvious areas of risk to company assets and trends or incidents of loss. However, security spending is often viewed as a cost centre, therefore receiving limited attention in comparison to examining business units for legislated compliance requirements and proactive profit generation. The model, at Principle 4, proposes that security compliance is audited and recognised as a long term revenue enhancer. Examining security with cost and benefit analysis provides opportunity in providing a balanced security plan which makes best use of people, technology and management to address significant risks.

Less than 30 per cent of the target population reported reference to security management in their corporate disclosures to company stakeholders, particularly shareholders. The model considers and implements security communications to company stakeholders in Principle5 and Principle 6, informing shareholders and potential investors that the company recognises its responsibilities in maintaining a secure and sustainable operating environment.

Management of significant business risks should include security risk in any holistic risk management plan for a public company. The model implements

security risk management at Principle 7 to ensure security is a component of recognising and managing business risk and ensuring internal control and compliance systems relate to security, alongside other significant risks.

No respondent company had a member of the board with any qualifications or experience in security management. Only a third of respondents had a member of the board or committee with designated responsibility for the security function. The model implements security induction and awareness information to existing or new directors and executive management under Principle 8 of encouraging enhanced performance. This supports security recognition and practice within the board and corporate culture.

This study demonstrates that the Corporate Governance Security Model has the potential to enhance current corporate governance practices. The model implements security to the corporate governance framework to formally recognise and promote effective management of security risk and compliance. Applying security risk management, as an applied business process supports and enhances the corporate reputation and compliments other risk and business management practices. Security of information and confidentiality is enhanced to encourage reports of misconduct within the company, generating a strong and inherent security culture.

Chapter 6

Study outcomes and recommendations

This chapter presents the outcomes and recommendations of the study which set out to determine if the *Corporate Governance Security Model* recognises an existing security function in current governance practices and if the model would enhance the governance framework.

Research Conclusions

A major finding of this study is that security functions and responsibilities are poorly recognised and documented by Australia's largest public company boards. Many directors will have no experience or qualifications in security management and this is likely to be reflected down through the organisation resulting in low to medium security awareness and culture.

Security functions are being limited to form part of internal controls within the operating environment and generally viewed as a cost centre which does not contribute to revenue. Security functions are not being holistically applied across the organisation or within the corporate governance or risk management framework.

Applying the survey results to the target population, namely ASX/S&P 200 companies, security is not recognised as a board responsibility. This should be disturbing to investors and the wider community as the current security environment presents significant risks, particularly with the backdrop of sustained terrorism and e-commerce threats. The literature review found that in most cases, in the event of a terrorist or major security event, the business community will not be knowledgeable about the roles, responsibilities or interactions of public health, safety, emergency and security agencies.

Corporate security threats to Australia's largest 200 companies can come from radical international organisations, domestic extremist groups, organised crime networks, competitors, company officers and employees. Companies must plan for a variety of attacks and events, and understand the governmental and risk management framework in place to respond to each event. Other responses include addressing personnel behaviour, health and safety, emotional distress and a plethora of business continuation issues (Business Executives, 2004).

If security risk management is not being formally recognised as a Board responsibility, investors should be asking Directors if these significant risks are being managed and addressed. If a company does recognise its security responsibilities and has policy in place, investors should be informed under current corporate governance guidelines, namely Principle 6. This enables the company's reputation and market position to be enhanced by communicating to

stakeholders that the company has considered its security for long term sustainability.

The application of the *Corporate Governance Security Model* was found to be a consistent and realistic guide for companies to formally introduce and apply security functions to corporate governance practices. The literature review found that the message from the top down must be that the company wants to develop and maintain a security culture. If the message is that the company recognises its need to develop security functions, security behaviour and a general security environment, and if the message is serious and sincere, then those things themselves become the focus for the conduct of organisational matters.

Most employees currently don't consider their security responsibility and have the mentality that security is someone else's problem, not theirs (Fitzgerald, 2004). This reflects a poor security culture in Australian business communities. Poor culture provides unnecessary vulnerability to company activities in the form of preventable security breaches and the inability to identify loss or incident trends, potentially exposing the company to significant liability. This is reiterated in the study's finding that there is a low application and documentation of formal security conduct and reporting systems within current governance frameworks.

Research recommendations

The results of this study were reasonably restricted to allow a number of conclusive results, however there are generally inconclusive results. There are a number of recommendations resulting from the study and are primarily concerned with the continued need for research into the application and recognition of security risk management within the hierarchy of executive and business management.

The first recommendation is for a similarly structured study to be conducted but with far greater support and recognition within the corporate sector to capture a substantive measure of the application and recognition of security risk management within the corporate governance framework. This would provide the Australian investment community with a real insight into the security and risk management standing and capability of Australia's largest companies to respond to current security risks and threats, in particular terrorism and information warfare.

A second recommendation involves a far greater assessment and analysis of the *Corporate Governance Security Model* and its application to corporate governance practices. The benefits of greater application of security awareness and recognition in corporate governance have remained relatively unmeasured and would require a longitudinal study or predictive research. It is envisaged that such a study would be inherently complex, involving an accurate assessment of

attitudes towards the security discipline as a corporate profession and necessity, and if this may vary over time.

It is recommended that aspects of this research be applied to current longitudinal studies which relate to security. The Australian Computer Crime and Security Survey, commenced in 2002, is conducted annually and addresses computer security management, vulnerabilities, threats and challenges. New longitudinal research in line with this study may be added to this survey to measure an increase in security recognition and security risk management in corporate governance practices.

Further research is strongly recommended in areas of corporate security culture, security awareness training and security risk communications. The poor recognition of security within corporate governance may be resultant from the inability of security managers to justify security as a long term revenue enhancer and they may be reinforcing the view that security is a cost centre which requires restrictive control.

With enhanced security risk communications and better security awareness training, security cultures can be developed to allow the benefits of reduced security incidents and company sustainability to be realised. Significantly improving an organisation's security culture may have a positive impact on improving corporate ethics and conduct, meaning security can have a far greater strategic and holistic benefit than is currently understood.

Finally, continued exploratory research is required into security risk management design, application and treatment options to introduce benchmark guidelines, such as in Australian Standards, in security management for corporate Australia.

Chapter 7

Conclusion

This study is based upon its implications to corporate governance and security risk management practices in Australia and overseas. The study researched security's application to the corporate governance and risk management framework, and created a model with which it can be implemented. The model endeavors to provide new approaches and guidance to current corporate governance policy, and promote security management as a valued business practice at the executive management and board level.

This research supports security risk management as a viable and necessary business framework that can contribute to core business and profit generation, however the study determined that the security function is poorly recognised in current corporate governance frameworks. If holistically applied, the *Corporate Governance Security Model* is likely to contribute to promoting best practice security management and supports security functions as a necessary contributor in corporate assessment, particularly risk management, auditing and business continuity.

Security functions in corporate governance can first be enhanced by the disclosure of its role and documented responsibility for the board of director's to apply strategic security direction for day-to-day management and internal

controls. The review of security practices, which have remained, unchanged or unchallenged may lead to better practices that maximise corporate value. At worst, an informed confidence is provided to the board and management about existing security management issues and trends.

Senior management experience is likely to become an important qualification as the role of security continues to emerge in corporate significance. Currently, security functions are mostly accommodated in mid-level management positions. The highest levels of the organisation, the Board of Directors and its operating committees must be provided with the strategy, costs and related impacts of the security function, and the nature and probability of catastrophic and significant security risk events. This allows greater compliance with current corporate governance principles and an informed investment community.

The application of security risk management to corporate governance should involve the board or designated committee formulating the security policy of the organisation and developing an appropriate security culture and awareness regime. Strategic security planning should be in line with corporate direction and key resources, directing the board and executive management in protecting all asset types, mitigating loss and providing accountability for corporate governance.

Strong holistic security controls which are reported regularly to the board, and audit and risk management committees should enable alert watch-keeping of

director, management and employee behaviour, critical infrastructure and asset protection strategies, operational security and loss mitigation, and monitoring of external threats and risks, all which can cause severe stress on short and long term financial performance.

Articulating and championing the business case for security management must be seen as an essential part of the role played by any corporate security director. This may be more difficult if security communications are insufficient and not directly reporting to top management or integrated into corporate practices and culture. However as security research continues and security management becomes more integrated into strategic management, this should improve.

References

Adekunle, A. (2002). Privatisation and the challenge of corporate governance in Nigeria. In MacMillan, F. (2002). *International Corporate Law Annual Vol 2.* Oregon: Hart Publishing. pp167 - 184.

Appleby, R. C. (1987). *Modern Business Administration.* London: Pitman Publishing.

AS/NZS 4360:1999. *Risk Management.*

ASIS International. (2004). Chief Security Officer Guideline.

ASX Corporate Governance Council (2003). *Principles of Good Corporate Governance and Best Practice Recommendations.* Australian Stock Exchange Limited.

ASX Guidance Note 9 (2001). *ASX Disclosure of Corporate Governance Practices: Listing Rule 4.10.* Australian Stock Exchange Limited.

Best, J.W. (1981). *Research in Education.* Sydney: Prentice-Hall.

Blades, A. and McClure, S. (2003). *Management of the Security Function: Guide.* Perth: Edith Cowan University.

Bosch, H. (2001). Introduction. In. *Collapse Incorporated: Tales, Safeguards and Responsibilities of Corporate Australia.* Sydney: CCH. pp. 1 – 7.

Bosch, H. (1995). *The Director at Risk: Accountability in the boardroom.* Pitman Publishing: Melbourne.

Broersma, M. (2004, July 16). Study: Company Execs admit IT Idiocy. *Techworld.com.* In. CSO online [on-line]. Available 21/08/2004 WWW: http://www.csoonline.com.au/index.php?id=1103755656&eid=-302

Buffini, F. (2004, March 11). Directors face even greater expectations. *Australian Financial Review.* [on-line]. Available WWW: http://afr.com/articles/2004/03/09/1078594355714.html Visited 19/09/2004.

Burgeat, E. (2001). Foreword. In. *Corporate Governance in Asia: A comparative perspective.* Organisation for Economic Co-operation and Development: Paris. pp. 3.

Business Executives for National Security. (2004, April). Company Primer on Preparedness and Response Planning for Terrorist and Bioterrorist Attacks. BENS Metro Atlanta Region: Homeland Security Advisory Group.

Cassidy, D. (2003). Maximizing shareholder value: the risks to employees, customers and the community. *Corporate Governance*. Vol. 3, No. 2. pp. 32 – 37.

Cavanagh, T. E. (2004a). *Corporate Security Management: Organisation and Spending since 9/11*. Research Report. The Conference Board.

Cavanagh, T. E. (2004b). *Security in Mid-Market Companies: The view from the top*. Executive Action Number 102, The Conference Board.

Clarke, F. and Dean, G. (2001). Corporate collapses analysed. In. *Collapse Incorporated: Tales, Safeguards and Responsibilities of Corporate Australia*. Sydney: CCH. pp. 71 - 98.

Cohen, L.and Manion, L. (1980). *Research methods in education*. London: Croom Helm.

Cohen, S. and Grace, D. (2001). Ethics and the sustainability of business. In. *Collapse Incorporated: Tales, Safeguards and Responsibilities of Corporate Australia*. Sydney: CCH. pp. 99 - 128.

Cole, C. (2004, August). Think your CEO is Honest? How would you know?! *Directors Monthly*, 28, 8. National Association of Corporate Directors: Washington.

Collier, P. (1997). Audit Committees in Smaller Listed Companies. In Keasey, K. and Wright, M. (Ed.), (1997). *Corporate Governance Responsibilities, Risks and Remuneration*. Chichester: John Wiley & Sons. pp. 93 - 119.

Cook, W. (2004, September 30). A Foreseeable Future. *CSO Online* [on-line]. Available WWW: http://www.csoonline.com.au/index.php?id=420533628&eid=-302. Visited 1/10/2004.

Corporations Act 2001 (Cth). s. 180 – 184.

Criminal Code Act 1995 (Cth) s. 12.3(6)

Cromie, A. (2004, September). How risk management adds value to business. *Company Director*, 20, 8. Australian Institute of Company Directors: Sydney.

Dang, J. (2000). *The Governance of Corporate Groups*. Cambridge University Press: London.

Dearne, K. (2003, April 3). Security Collaboration Needed: AG. *Australian IT*. [on-line]. Available WWW: http://australianit.news.com.au/articles/0,7204,6228459%5e15319%5e%5enbv%5e15306,00.html

Dobbie, M. (2004, September). Bull's Eye: How to pick winning stocks. *Shares*. pp. 25 – 28.

Duncan, K., Gale, S., Tofflemore, J. and Yaksick, R. (1992). Conceptualizing a Value-Added Approach to Security Management: The Atkinson Security Project I. *Security Journal*, Vol. 3, No. 1., pp. 4 – 13.

Dunk, A. and Kilgore. A. (1998). Financial markets, corporate governance, and short-term pressures in Australia. In Demirag, I.S. (Ed.). (1998). *Corporate governance, accountability, and pressures to perform: An international study*. London:JAI Press. pp. 141 - 161.

Dunlop, I.T. (2001). Latest Directions in Corporate Governance. In. *Corporate Governance in Asia: A comparative perspective*. Organisation for Economic Co-operation and Development: Paris. pp. 43 - 54.

Economic Crime Survey (2003). PriceWaterHouseCoopers.

ECU Policies and Procedures. (1998). *Conduct of Ethical Research Involving Humans*. Available WWW: http://www.ecu.edu.au/GPPS/assets/pdfs/ac023.pdf Visited 11/06/2005.

Ellett, F. (2000) Australia and the UK on the quest for best corporate governance practice. In MacMillan, F. (2000). *International Corporate Law Annual Vol 1*. Oregon: Hart Publishing. pp. 171 – 178.

Elliott, G. (2003, 8 October). Gloves off in board war: Shareholders attack executives over pay disclosure. *The Australian*. pp. 33.

Eyers, J. (2004, March 11). A culture of best practice beats regulation. *Australian Financial Review*. [on-line]. Available WWW: http://afr.com/articles/2004/03/09/1078594355735.html Visited 19/09/2004.

Fishel, D. (2003). *The Book of the Board: Effective governance for non-profit organisations*. Sydney, The Federation Press.

Fitzgerald, M. (2004, August 12). How to stop a laptop thief. *CSO online* [on-line]. Available 21/08/2004 WWW: http://www.csoonline.com.au/index.php?id=1973406143&eid=-302

Fenton-Jones, M. (2004, March 11). Finance collapses around the work force change. *Australian Financial Review*. [on-line]. Available WWW: http://afr.com/articles/2004/03/09/1078594355732.html Visited 19/09/2004.

Fenton-Jones, M. (2003, 14 October). Internet fraud a risk for business. *Australian Financial Review.* pp. 47.

Ferguson, A. (2003). Skewed Priorities. *BRW.* pp. 35 - 40.

Gengler, B. (2003, 4 November). Crime fight focus shifts to espionage. *The Australian.* pp. 7.

Gettler, L. (2004, September 15). CFO's dismiss new risk rules. *The West Australian.* p. 42.

Gurdon, Z.A. (2001). *Socialisation and the Security Function: Defining a positive role for security in the socialisation of new employees.* Honours Thesis (unpublished). Edith Cowan University: Perth.

Hamilton, K. (2004, March 11). We have many shining examples to be proud of. *Australian Financial Review.* [on-line]. Available WWW: http://afr.com/articles/2004/03/09/1078594355708.html Visited 19/09/2004.

Hansell, C. (2003). *What directors need to know: Corporate Governance.* Carswell: Torronto.

Harper, I.R., Keller, J.G. and Pfeil, C.M. (2000). Does Risk Management make Financial Markets Riskier? In. Frenkel. M, Hommel, U and Rudolf. M (2000). Eds. *Risk Management: Challenge and Opportunity.* Springer-Verlag: Berlin. pp. 5.

Hayes, J. and Truscott, J. (2004, May/June). The integration of risk, safety and security. *Security Oz Magazine.* No. 29. pp. 36 – 39.

Jain, A.K. (2000). Governance of Global Financial Markets: Risk of Hubris. In. Frenkel. M, Hommel, U. and Rudolf. M. (2000). Eds. *Risk Management: Challenge and Opportunity.* Springer-Verlag: Berlin. pp. 231.

Kaen, F.R. (2000). Risk Management, Corporate Governance and the Modern Corporation. In. Frenkel. M, Hommel, U. and Rudolf. M. (2000). Eds. *Risk Management: Challenge and Opportunity.* Springer-Verlag: Berlin. pp. 247.

Kuada, J. and Gullestrup, H. (1998). Cultural Context in Corporate Governance. In Demirag, I.S. (Ed.). (1998). *Corporate governance, accountability, and pressures to perform: An international study.* London:JAI Press. pp. 25 – 56.

Lawson, M. (2004, April 7). Be serious, you can't take risks. *Australian Financial Review.* [on-line]. Available WWW: http://afr.com/articles/2004/04/06/1081222459146.html Visited 19/09/2004.

Legard, D. (2004, September 16). Online Fraud: We got law, but no enforcement. *IDG News Service*. [on-line] Available WWW: http://www.computerworld.com.au/index.php?id=134758276&eid=-44 Visited 19/09/2004.

Main, A. (2003). *Other people's money: The complete story of the extraordinary collapse of HIH*. Sydney: HarperCollins Publishers.

McClure, S.A. (1997). *Security Decay: The erosion of effective security*. Honours Thesis (unpublished). Edith Cowan University: Perth.

McCrie, R. D. (2001). *Security Operations Management*. London, Butterworths-Heinemann.

McGeough, P. (2004, September 11). We must all share blame for the madness of terror attacks. *The West Australian*. pp. 44 – 45.

Mills, K. (2003, 23 September). US fraud laws will make a big imprint on local tech firms. *The Australian IT Business*, p. 1, 4.

Mills, R.W. (1997). Internal Control Practices within Large UK Companies. In Keasey, K. and Wright, M. (Ed.), (1997). *Corporate Governance Responsibilities, Risks and Remuneration*. Chichester: John Wiley & Sons. pp. 121 – 143.

Moullakis, J. (2004, 9 January). Banks criticised over hoax emails. *Australian Financial Review*. pp. 5.

Mroz, E. and Conner, B. (2003, 17 November). Business has to enlist in this war. *International Herald Tribune*. pp. 6.

Nadler, D.A. (2004, September). Increasing director performance. *Company Director*, 20, 8. Australian Institute of Company Directors: Sydney. pp. 8-14.

Nam, I.C., Kang, Y. and Kim, J.K. (2001). Comparative Corporate Governance Trends in Asia. In. *Corporate Governance in Asia: A comparative perspective*. Organisation for Economic Co-operation and Development: Paris. pp. 85 - 119.

Pausenberger, E. and Nassauer, F. (2000). Governing the Corporate Risk Management Function: Regulatory Issues. . In. Frenkel. M, Hommel, U and Rudolf. M (2000). Eds. *Risk Management: Challenge and Opportunity*. Springer-Verlag: Berlin. pp. 265.

Pitsis, S. (2004, 9 January). Hole in security upgrade at ports. *The Australian*. pp. 4.

Png, C. (2001). *Corporate Liability; A study in principles of attribution.* The Hague: Kluwer Law International.

Pownall, M. (2004, September 9-15). Boards under the microscope. Western Australian Business News. pp. 14-15.

Quirke, B. (1996). *Communicating Corporate Change: A practical guide to Communication and Corporate Strategy.* McGraw-Hill Companies: London.

Rohde, L. (2004). Gartner analysts point out the security you don't need. IDG News Service. [on-line]. Available WWW: http://www.csoonline.com.au/index.php?id=2113312780&eid=-302 Visited 21/09/2004.

Sarre, R. (2001). Risk Management and regulatory weakness. In. *Collapse Incorporated: Tales, Safeguards and Responsibilities of Corporate Australia.* Sydney: CCH. pp. 291 - 323.

Sekaran, U. (1992). *Research methods for business.* 2Ed. New York: John Wiley & Sons.

The Economist. (2004, July 24). Nuclear Weapons Research: Yet another breach. pp. 67.

Tschoegl, A.E. (2000). The key to Risk Management: Management. In. Frenkel. M, Hommel, U and Rudolf. M (2000). Eds. *Risk Management: Challenge and Opportunity.* Springer-Verlag: Berlin. pp. 104.

Vijayan, J. (2004, September 27). E-Business sites hit with attacks, extortion threats. Computerworld. [on-line]. Available WWW: http://www.csoonline.com.au/index.php?id=739018247&eid=-302 Visited 1/10/2004

Walter, I. (2000). The Relevance and Management of Reputation Risk in the Global Securities Industry. In. Frenkel. M, Hommel, U and Rudolf. M (2000). Eds. *Risk Management: Challenge and Opportunity.* Springer-Verlag: Berlin. pp. 25.

White, A. (2001). Flow on Effects of Recent Collapses. In. *Collapse Incorporated: Tales, Safeguards and Responsibilities of Corporate Australia.* Sydney: CCH. pp. 41-70.

Williams, C. (2003, 16 October). Greater security needed to protect businesses. *Canberra Times.* pp. 13.

Yates, A. (2004). *Thematic research priorities for the protection of the built environment including critical infrastructure: An industry perspective.* Canberra: Institution of Engineers.

Yates, A. (2003). *Will industry's investment in protecting its critical infrastructure be sufficient.* Engineers Australia: Canberra.

Bibliography

ANAO (2001). *An Analysis of the Chief Financial Officer Function in Commonwealth Organisations: Benchmarking Study.* Canberra: The Auditor General.

ANAO (2003). *Management of Risk and Insurance.* Canberra: The Auditor General. Report No. 3.

Ansell, J. and Wharton, F. (1992). *Risk: Analysis, Assessment and Management.* Cichester: John Wiley & Sons.

Brewer, J.D. (2000). *Ethnography.* Buckingham: Open University Press.

Bushell, S. (2003). "State of the CIO 2003." *CIO Magazine.*

Cunningham, W.C., Strauchs, J.J., and Van Meter, C.W. (1990). *Private Security Trends 1970 – 2000: The Hallcrest Report II.* Boston: Butterworth-Heinemann.

Croall, H. (2003). Combating Financial Crime: Regulatory versus Crime Control Approaches. *Journal of Financial Crime.* Vol 11, No. 1. pp. 45 – 55.

Cutting, B. and Kouzmin, A. (2002). Evaluating corporate board cultures and decision making. *Corporate Governance.* Vol 2. No. 2. pp. 27 – 45.

Denzin, N.K. (1970). *Sociological Methods: A Sourcebook.* Chicago: Aldine Publishing Company.

Duncan, K., Gale, S., Tofflemore, J. and Yaksick, R. (1992). An Implementation of the Atkinson Model: The Atkinson Security Project III. *Security Journal,* Vol. 3, No. 1., pp. 27 - 44.

Duncan, K., Gale, S., Tofflemore, J. and Yaksick, R. (1992). The ASIS Foundation Benchmark II Survey Study. *Security Journal,* Vol. 3, No. 1., pp. 45 - 56.

Fisse, B. and Braithwaite, J. (1993). *Corporations, Crime and Accountability.* Cambridge: Cambridge University Press.

Ghauri, P.N., Gronhaug, K. and Kristianslund, I. (1995). *Research methods in business studies: A practical guide.* London: Prentice Hall.

Gill, J. and Johnson, P. (1997). *Research methods for managers* (2nd Ed.). London: Paul Chapman Publishers.

Gunter, B. and Furnham, A. (2001). *Assessing Business Potential: A Biodata approach*. London: Whurr Publishers.

Hussey, J. and Hussey, R. (1997). *Business Research: A practical guide for undergraduate and postgraduate students*. London: MacMillan Press.

Ietto-Gillies (2002). *Transnational Corporations: Fragmentation amidst Integration*. London, Routledge.

Martin, J.D. and Petty, J.W. (2000). *Value Based Management: The Corporate Response to the Shareholder Resolution*. Boston, Harvard Business School Press.

Mills, G. (1981). *On the Board*. Hampshire: Gower Publishing Company.

Miner, J. B., Ed. (1995). *Administrative and Management Theory*. Vermont, Dartmouth Publishing Company.

Mitchell, M. and Jolley, J. (1988). *Research Design Explained*. Orlando: Holt, Rinehart and Winston, Inc.

Monks, R.A.G. and Minow, N. (1995). *Corporate Governance*. Oxford: Blackwell Publishers.

Scherrer, P.S. (2003). Management turnarounds: diagnosing business ailments. *Corporate Governance*. Vol. 3. No. 4. pp. 52 – 62.

Smith, B., Ed. (1992). *Management Development in Australia*. Sydney, Harcourt Brace Jovanovich Publishers.

Ward, R.D. (1997). *21st Century Corporate Board*. New York: John Wiley & Sons.

Zandsrta, G. (2002). Enron, board governance and moral failings. *Corporate Governance*. Vol 2. No. 2. pp. 16 – 19.

Annexure 1

Letter of Approach for questionnaire

SUBJECT: National Corporate Governance & Security Study

Your assistance is sought in a national research project to identify the role of security in corporate governance. The study forms part of a security science thesis for Edith Cowan University, Perth. A verification letter for this research is available from ECU upon request. As you may appreciate conducting security related research is difficult due to potential sensitivities. Any assistance you are able to provide would be greatly appreciated.

The significance of this study is based upon its implications to current corporate governance and security management practices in Australia and overseas. Should the study confirm security's enhancement of the corporate governance framework, and a model with which it can be implemented, it will provide new approaches to current corporate governance policy, and promote security as a valued business practice at executive management and board level.

The research involves the application of a security model for corporate governance practices and seeks your responses to a questionnaire. The questionnaire aims to identify a security function in your corporate governance practices and consists of only 19 questions. Areas for consideration are;

1. Recognition of an existing security function in corporate governance;
2. Recognition of security management qualifications or experience;
3. Response to changes in the security environment; and
4. Acknowledgment of applied security functions in corporate governance practices.

You represent a listed company on the Australian Stock Exchange and in the S&P/ASX200 as of 1 May 2004. Your responses will significantly benefit the study and will be kept anonymous within the thesis. If you wish to clarify any issue or discuss this research further, please do not hesitate to contact Chris directly on 0432 743 261.

To participate in the survey, please visit http://www.soem.ecu.edu.au/~ccubbage/

Sincerely,

Chris Cubbage

Annexure 2

National Survey of Security in Corporate Governance

Introduction

Your participation in this study will contribute to the research of corporate governance, security and risk management in Australian business. The aim of this questionnaire is to determine the application of a security function in your corporate governance practices.

You represent a listed company on the Australian Stock Exchange ('ASX') and within the S&P/ASX200 as of 1 May 2004. The target is to achieve 30%, equaling 60 respondents.

Your information is valued and will be kept anonymous within the thesis. Some companies may be discussed as a case study, however only publicly available information will be used.

Thank you.

Start Questionnaire ***Purpose of the study***

Significance of the study

Purpose of the study

Thematic research priorities for the protection of the built environment, including critical infrastructure, proposed by Yates (2004, p. 10), state that challenges related to business awareness of the changed security environment and risk management include;

g) A failure to integrate security considerations into governance frameworks;
h) Lack of business awareness that sound business risk management, security and resilience can be a long term revenue enhancer;
i) Lack of benchmarks and metrics for effective security investment;
j) Lack of integration of security into the issues of consideration for all professionals and managers;
k) Lack of risk management and security risk experience in business; and
l) Lack of modeling tools and validation models.

This study is in line with Yates' research priorities by proposing research into security's application to essential corporate governance principles recommended by the ASX Corporate Governance Council (2003). By demonstrating that security enhances corporate governance, it supports security as a viable and necessary business framework that can contribute to core business and profit generation. The development of a security model for corporate governance promotes best practice security management and supports security as a contributor in areas such as corporate assessment, particularly risk management, auditing and business continuity.

Start Questionnaire

Significance of the study

This study is significant and well timed as corporate governance and security are two of the major issues concerning the corporate world today. The two issues are brought together in this study.

The significance of this study is based upon its implications to current corporate governance and security management practices in Australia and overseas. Should the study confirm security's enhancement of the corporate governance framework, and a model with which it can be implemented, it will provide new approaches to current corporate governance policy, and promote security as a valued business practice at executive management and board level.

The study will also generate more interest in security management research and education, particularly in its application to business leadership and executive management. This will contribute to the continued growth of the security profession.

Start Questionnaire

Questionnaire

Please answer the following questions by selecting from the drop down menu.

Part 1 Recognition of an existing security function in Corporate Governance

a) Is your organisation's security documented as a board responsibility?

---

b) Is your organisation's security documented as an audit committee responsibility?

---

c) Does the organisation include security in its review of internal controls?

---

d) Does the company integrate security policy with corporate governance policy?

---

e) Does your company have a policy promoting a security culture?

Part 2 Recognition of security management qualifications or experience

a) Does any member of the board or senior executive have qualifications or demonstrated experience in security management?

---

b) Does any member of the board or an appointed committee have designated responsibility for security management?

c) Has the board or an appointed committee sought external advice regarding a security related issue within the last 2 years?

---

d) Do you consider that corporate security advice is available?

---

e) Would you consider obtaining independent security advice?

Part 3 Response to changes in security environment

a) Have you recognised changes in the security environment which have increased your business risk within the last 5 years?

---

b) Do you consider that the current security environment presents significant business risks to your company?

---

c) Has the board or an appointed committee reviewed security policy within the last 2 years?

---

d) Has the board or an appointed committee audited security procedure within the last 2 years?

---

e) Has the board or an appointed committee been informed of an internal security event or incident in the last 12 months?

Part 4 Acknowledgment of applied security functions in corporate governance practices

a) Do you regard good security practices as part of good corporate governance?

---

b) Do you consider that corporate governance is, or would be, enhanced by the application of a security function?

---

c) Do you consider that an application of a security function to corporate governance contributes to long term revenue enhancement?

---

d) Do you consider that company stakeholders would favour disclosure of a security function within corporate governance disclosures?

Thank you for your time.

A copy of the study and results will be forwarded to you upon completion.

Annexure 3 - CORPORATE GOVERNANCE SECURITY MODEL

Governance Principle	Governance Practice	Security Function Applied	Outcome/Disclosure Statement
Principle 1: Lay solid foundations for management and oversight	Formal board charter that details the functions and responsibilities of the board	Security is included as a responsibility of the board within its current responsibility to review and ratify systems of risk management and internal compliance and control	The board recognises its responsibility for security risk management and security compliance and control
Principle 2: Structure the board to add value	All directors should bring an independent judgment to bear in decision making with procedures in place to take independent professional advice if necessary	Professional security advice is made available to the board and directors in addition to other professions.	The board accepts security as a profession and seeks specialist advice on security issues when necessary
Principle 3: Promote ethical and responsible decision-making	1) Adherence to a documented Code of Conduct 2) Adherence to a documented trading policy	1) Adherence to security policy and procedures is recognised within the Code of Conduct 2) A formal response within security guidelines to prohibited trading and unethical conduct	Security risk management is recognised and practiced within the board and corporate culture
Principle 4: Safeguard integrity in financial reporting	Existence of an independent audit committee; • The committee should report to the board all matters relevant to the results of its review of risk management and internal compliance and control systems	Security compliance is audited and results are reported to the board	Security risk management is maintained, monitored and reviewed by the board Security management is recognised by the board as a long term revenue enhancer

Governance Principle	Governance Practice	Security Function Applied	Outcome
Principle 5: Make timely and balanced disclosure	Continuous disclosure policies and procedures are in place; • Internal notification and decision making concerning the disclosure obligation • Safeguarding confidentiality of corporate information to avoid premature disclosure	Security implications are considered by the board in making 'sensitive' disclosures	Security related risks are managed for disclosure of 'sensitive' information
Principle 6: Respect the rights of shareholders	Publishing the company's policy on shareholder communication will help investors to access the information; Companies are encouraged to maintain a company website and communicate with shareholders via electronic means.	Security implications or issues are considered by the board in its communications with shareholders, particularly with electronic communications	Shareholders are ensured that the company's electronic communications are secure and that electronic integrity is maintained
Principle 7: Recognise and manage risk	The Board or appropriate board committee should establish policies on risk oversight and management. This should include policies on oversight, risk profile, risk management, compliance and control, and assessment of effectiveness.	The board accepts security risk management as a component of recognizing and managing business risks The board determines security policy and internal security compliance and control systems	Security risk management is maintained, monitored and reviewed by the board Security management is recognised by the board as a long term revenue enhancer

Governance Principle	Governance Practice	Security Function Applied	Outcome
Principle 8: Encourage enhanced performance	An induction program should be made available to new directors to gain an understanding of the company's financial, strategic, operational and risk management position; the role of the board committees; and their rights, duties and responsibilities	Security induction and awareness information is provided to new directors and executive management	Security risk management is recognised and practiced within the board and corporate culture
Principle 9: Remunerate fairly and responsibly	Disclosing the remuneration policy provides a transparent and readily understandable framework for executive compensation.	Model not applied	Model not applied
Principle 10: Recognise the legitimate interests of stakeholders	Establish and disclose a code of conduct to guide compliance with legal and other obligations to legitimate stakeholders; A code of conduct should enable employees to alert management and the board in good faith to potential misconduct without fear of retribution, and should require recording and investigation of such alerts; The company should have a system for ensuring compliance with its code of conduct and for dealing with complaints	Effective management of security risk and compliance enhances the corporate reputation and compliments other risk management practices; Security of information and confidentiality is enhanced to encourage reports of misconduct; Security has a response capacity, including investigative, to deal with misconduct and compliance issues.	Security risk management is recognised and practiced within the board and corporate culture

Annexure 4 - Document analysis of ASX listed companies

60 S&P/ASX 200 listed companies, May 1, 2004

	Company Information		Document Reference		Document Analysis - Annual Report 2001/2002 and Disclosure Documents							
	ASX Code	Home Page	Annual Report	Sector	Respondent Contact	Audit Committee	Risk Management Committee	Environmental Risks	OH&S Risks	Asset Protection	Security Function	Reporting Policy
1	AFI	http://www.afi.com.au/	Annual Report 2002	Financials Ex Property	Fergus Ryan	Yes	Yes	No	No	No	No	No
2	AGG	http://www.anglogold.com/	Annual Financial Statements 2003	Materials	R. Godsell	Yes	No	Yes	Yes	No	No	Yes
3	AGL	http://www.agl.com.au/AGLNew/default.htm	Annual Report 2003	Utilities	C. Hewson	Yes	Yes	Yes	Yes	Yes	No	No
4	ALN	http://www.alinta.net.au/	Annual Report 2003	Utilities	F Harris	Yes	Yes	Yes	Yes	No	Yes	No
5	AMC	http://www.amcor.com/	Concise Report 2003	Materials	R. Barton	Yes	No	Yes	Yes	Yes	No	No
6	ANZ	http://www.anz.com/default.asp	Corporate Governance Policy	Banks	J. Ellis	Yes	Yes	Yes	Yes	No	No	Yes
7	ARQ	http://www.arcenergy.com.au/	Corporate Governance Statement	Energy	Graham Riley	Yes	No	Yes	Yes	No	No	No
8	ASX	http://www.asx.com.au/	Corporate Governance Statement	Diversified Financials	Catherine Walter	Yes	Yes	No	Yes	Yes	Yes	No
9	BBG	http://www.billabongcorporate.com/	Corporate Governance Statement	Consumer Durables & Apparel	Allan Macdonald	Yes	No	Yes	Yes	No	No	No
10	CBA	Commonwealth Bank Group	Corporate Governance	Banks	J. Schubert	Yes	Yes	Yes	Yes	No	No	Yes
11	CML	http://www.colesmyer.com/	Statement of Principles	Food & Drug Retailing	Tony Hodgson	Yes	No	Yes	Yes	No	No	No
12	COH	http://www.cochlear.com.au/	Corporate Governance	Health Care Equipment & Services	Carol Holley	Yes	Yes	Yes	Yes	Yes	Yes	Yes
13	CSM	http://www.consminerals.com.au/	Annual Report 2003	Materials	Colin Smith	Yes	No	Yes	Yes	No	No	Yes
14	CSR	http://www.csr.com.au/	Corporate Governance Statement 2003	Materials	Carolyn Hewson	Yes	No	Yes	Yes	No	No	Yes
15	CTX	http://www.caltex.com.au/	Corporate Governance Practices	Energy	Elizabeth Bryan	Yes	No	Yes	Yes	No	No	No
16	EQI	http://www.equigold.com.au/	Annual Report 2003	Materials	S.Lee	Yes	No	Yes	Yes	Yes	No	No
17	ERA	http://www.energyres.com.au/	Corporate Governance Statement	Materials	Dr B. Hickman	Yes	No	Yes	Yes	Yes	Yes	Yes
18	FGL	http://www.fosters.com.au/	Annual Report 2003	Food Beverage & Tobacco	G. McGregor	Yes	No	Yes	Yes	No	No	Yes
19	FLT	http://www.flightcentre.com.au/	Insufficient on line information	Hotels Restaurants & Leisure								
20	FOA	http://www.fal.com.au/	Annual Report 2003	Food & Drug Retailing	Sir Colin Maiden	Yes	No	Yes	Yes	No	No	No
21	HIG	http://www.highlandspacific.com/	Annual Report 2003	Materials	AJ Barry	Yes	No	Yes	Yes	No	No	No
22	HLY	http://www.hillsmotorway.com.au/	Corporate Governance Statement	Transportation	Mr Peter Byers	Yes	No	Yes	Yes	No	No	No
23	HVN	http://www.harveynorman.com.au/	Annual Report 2003	Retailing	Arthur Brew	Yes	No	Yes	Yes	Yes	Yes	Yes
24	IAG	http://www.iag.com.au/	Corporate Governance Statement	Insurance	Rowan Ross	Yes	Yes	Yes	Yes	Yes	Yes	Yes
25	KCN	http://www.kingsgate.com.au/	Annual Report 2003	Materials	John Falconer	Yes	No	Yes	Yes	No	No	No
26	KIM	http://www.kimberleydiamondco.com.au/	Annual Report 2003	Materials	Peter Danchin	No	No	Yes	No	No	No	No
27	LEI	http://www.leighton.com.au/	Corporate Governance Statement 2003	Capital Goods	D. Robinson	Yes	No	No	No	No	No	Yes
28	LLC	http://www.lendlease.com.au/	Annual Report 2003	Real Estate	G. Edington	Yes	Yes	Yes	Yes	No	No	No
29	LNN	http://www.lion-nathan.com/	Annual Report 2002	Food, Beverage & Tobacco	Gavin Walker	Yes	No	Yes	Yes	No	No	No
30	LSG	http://www.lionselection.com.au/	Annual Report 2003	Diversified Financials	Ewen Tyler	Yes	No	Yes	No	No	No	No
31	MAP	http://www.macquarie.com.au/map	Corporate Governance Statement	Transportation	Michael Lee	Yes	Yes	Yes	Yes	Yes	Yes	No
32	MAY	http://www.maynegroup.com/	Annual Report 2003	Health Care Equipment & Services	Peter Mason	Yes	No	Yes	Yes	No	No	No
33	MCC	http://www.macarthurcoal.com.au/	Corporate Governance Statement	Materials	Don Nissan	Yes	Yes	Yes	Yes	Yes	Yes	Yes
34	NFD	http://www.nationalfoods.com.au/	Corporate Governance Statement 2003	Food, Beverage & Tobacco	Doug Curlewis	Yes	Yes	Yes	Yes	No	No	Yes
35	NUF	http://www.nufarm.com/	Annual Report 2003	Materials	Graeme McGregor	Yes	No	Yes	Yes	No	No	No
36	NVS	http://www.novuspetroleum.com/	Corporate Governance Statement	Energy	Steve Mann	Yes	No	Yes	Yes	Yes	Yes	Yes
37	ORG	http://www.originenergy.com.au/	Corporate Governance Statement	Energy	Dr Helen Nugent	Yes	Yes	Yes	Yes	No	No	No
38	ORI	http://www.orica.com/	Corporate Governance Statement	Materials	Peter Duncan	Yes	Yes	Yes	Yes	Yes	Yes	Yes
39	OSH	http://www.oilsearch.com/html/	Corporate Governance Statement	Energy	J. Stitt	Yes	Yes	Yes	Yes	Yes	Yes	Yes
40	OST	http://www.onesteel.com/	Corporate Governance	Materials	D. Meiklejohn	Yes	No	Yes	Yes	No	No	No
41	PBL	http://www.pbl.com.au/	Corporate Governance	Media	Richard Turner	Yes	No	Yes	Yes	No	No	No
42	PDG	http://www.placerdome.com/	Corporate Governance	Materials	Robert Franklin	Yes	No	No	Yes	Yes	Yes	Yes
43	PMM	http://www1.portman.com.au/	Corporate Governance	Materials	Fiona Harris	Yes	Yes	Yes	Yes	Yes	No	No
44	PRK	http://www.patrick.com.au/	Corporate Governance	Transportation	E.Cloney	Yes	No	No	No	No	No	No
45	QAN	http://www.qantas.com.au/	Corporate Governance	Transportation	Margaret Jackson	Yes	No	Yes	Yes	Yes	Yes	Yes
46	RIO	http://www.riotinto.com/default.aspx	Annual Report 2003	Materials	David Mayhew	Yes	No	Yes	Yes	No	No	No
47	SEV	http://www.seven.com.au/	Annual Report 2003	Media	Prof. Murray Wells	Yes	Yes	No	Yes	No	No	No
48	SGW	http://www1.sog.com.au/	Corporate Governance	Materials	Thomas Lang	Yes	Yes	Yes	Yes	No	No	No
49	SHL	http://www.sonichealthcare.com/sonic/internet/	Corporate Governance	Health Care Equipment & Services	Dr Colin Goldschmid	Yes	Yes	Yes	Yes	No	No	No
50	SPT	http://www.spotless.com.au/	Annual Report 2003	Commercial Services & Supplies	Lawrence O'Bryan	Yes	No	No	No	No	No	No
51	TAB	http://www.tablimited.com.au/news.asp?NCID=1	Annual Report 2003	Hotels Restaurants & Leisure	B. Hutchinson	Yes	No	Yes	Yes	No	Yes	No
52	TEN	http://www.tencorporate.com.au/	Annual Report 2003	Media	Paul Gleeson	Yes	No	Yes	Yes	No	No	No
53	TLS	http://telstra.com/index.isp	Corporate Governance	Telecommunication Services	Bill Scales	Yes	No	Yes	Yes	Yes	Yes	Yes
54	TOL	http://www.toll.com.au/	Annual Report 2003	Transportation	R. Dunning	Yes	Yes	Yes	Yes	No	No	No
55	VBA	http://www.virginblue.com.au/	Corporate Governance	Transportation	Not Known	Yes	No	Yes	Yes	No	Yes	Yes
56	WAN	http://www.thewest.com.au/	Annual Report 2003	Media	P. Mansell	Yes	Yes	No	No	No	No	No
57	WMR	http://www.wmc.com/	Annual Report 2003	Materials	Adrienne Clarke	Yes	No	Yes	Yes	No	No	No
58	WOW	http://www.woolworthslimited.com.au/	Annual Report 2003	Food & Drug Retailing	L. L'Huillier	Yes	No	Yes	Yes	No	No	Yes
59	WPL	http://www.woodside.com.au/	Corporate Governance	Energy	Jillian Broadbent	Yes	Yes	Yes	Yes	No	No	No
60	ZFX	http://www.zinifex.com/Main.aspx	Corporate Goverance	Materials	Greig Gailey	Yes	No	Yes	Yes	No	No	Yes